HiPER 500 系列产品
高级配置手册

上海艾泰科技有限公司
http://www.utt.com.cn

版权声明

版权所有©2000-2010，上海艾泰科技有限公司，保留所有权利。

本文档所提供的资料包括 URL 及其他 Internet Web 站点参考在内的所有信息，如有变更，恕不另行通知。

除非另有注明，本文档中所描述的公司、组织、个人及事件的事例均属虚构，与真实的公司、组织、个人及事件无任何关系。

本手册及软件产品受最终用户许可协议（EULA）中所描述的条款和条件约束，该协议位于产品文档资料及软件产品的联机文档资料中，使用本产品，表明您已经阅读并接受了 EULA 中的相关条款。

遵守所生效的版权法是用户的责任。在未经上海艾泰科技有限公司明确书面许可的情况下，不得对本文档的任何部分进行复制、将其保存于或引进检索系统；不得以任何形式或任何方式（电子、机械、影印、录制或其他可能的方式）进行商品传播或用于任何商业、赢利目的。

上海艾泰科技有限公司拥有本文档所涉及主题的专利、专利申请、商标、商标申请、版权及其他知识产权。在未经上海艾泰科技有限公司明确书面许可的情况下，使用本文档资料并不表示您有使用有关专利、商标、版权或其他知识产权的特许。

艾泰®、UTT®文字及相关图形是上海艾泰科技有限公司的注册商标。

HiPER®文字及其相关图形是上海艾泰科技有限公司的注册商标。

此处所涉及的其它公司、组织或个人的产品、商标、专利，除非特别声明，归各自所有人所有。

产品编号（PN）：0900-0400-002

文档编号（DN）：PR-PMMU-1104.33-PPR-CN-1.1A

目 录

导 读 1

0.1 手册说明 1
0.2 界面风格 1
0.3 基本约定 1
0.3.1 列表功能详解 1
0.3.1.1 可编辑列表 2
0.3.1.2 只读列表 2
0.3.1.3 列表排序功能 3
0.3.2 符号约定 3
0.3.3 键盘操作约定 3
0.3.4 其他表达约定 4
0.4 出厂配置 4
0.5 内容简介 5

第 1 章 产品概述 8

1.1 关键特性 8
1.2 主要特点 9
1.3 规格 10

第 2 章 硬件安装 11

2.1 安装准备 11
2.2 安装流程 11
2.3 安装步骤 12
2.3.1 HiPER510 安装步骤 12
2.3.2 HiPER520 安装步骤 13

第 3 章 快速配置 16

3.1 配置正确的网络设置 16
3.2 开始菜单 18
3.2.1 登录设备 18
3.2.2 线路配置上网 19
3.2.3 不可不防 20
3.2.3.1 双线路路由配置 20
3.2.3.2 病毒防御 21
3.2.4 端口映射 21
3.2.5 系统信息 21
3.2.5.1 页面刷新功能 21
3.2.5.2 系统运行时间 22
3.2.5.3 系统资源状态 22
3.2.5.4 系统版本信息 23

3.2.5.5 系统端口状态 23
3.3 快捷图标 24
第 4 章 快速向导 25
4.1 快速向导 25
4.1.1 上网接入方式设置 25
4.1.2 上网接入线路配置 26
4.1.2.1 上网接入线路配置的注意事项 26
4.1.2.2 PPPoE 拨号上网配置 26
4.1.2.3 固定 IP 接入配置 28
4.1.2.4 动态 IP 接入配置 29
4.1.3 小结 30
第 5 章 基本配置 31
5.1 线路配置 31
5.1.1 线路连接信息列表 31
5.1.1.1 参数涵义 32
5.1.1.2 列表功能 33
5.1.1.3 PPPoE 拨号接入线路的拨号与挂断 34
5.1.1.4 动态 IP 接入线路的更新与释放 35
5.1.2 线路配置 35
5.1.2.1 PPPoE 拨号上网配置 36
5.1.2.2 固定 IP 接入配置 38
5.1.2.3 动态 IP 接入配置 39
5.1.2.4 删除线路 40
5.1.3 相关的缺省路由 41
5.2 线路组合 42
5.2.1 线路组合功能介绍 42
5.2.1.1 线路组合方式 42
5.2.1.2 线路检测机制 42
5.2.2 多线路负载均衡功能介绍 43
5.2.2.1 根据源 IP 地址指定优先线路 43
5.2.2.2 根据线路带宽合理分配流量 43
5.2.2.3 提供两种流量分配规则 44
5.2.3 线路组合通用设置 44
5.2.3.1 所有线路负载均衡 45
5.2.3.2 部分线路负载均衡，其余备份 45
5.2.4 线路检测及权重配置 46
5.2.5 线路组合信息列表 47
5.2.5.1 部分参数涵义 47
5.2.5.2 列表功能 48
5.2.6 配置线路组合 48
5.2.6.1 线路组合的配置顺序 48
5.2.6.2 线路组合通用设置配置步骤 48
5.2.6.3 线路检测及权重配置步骤 49

5.2.7 相关的检测路由 49
5.3 DHCP 和 DNS 服务器 50
5.3.1 DHCP 服务配置 50
5.3.2 DHCP 地址池使用信息 51
5.3.3 配置 DHCP 服务器 52
5.4 接口配置 53
5.4.1 接口配置 53
5.4.2 接口配置信息列表 54
5.4.3 配置 IP 地址 54
5.4.4 配置 MAC 地址 54
5.4.5 配置以太网工作模式 55
5.5 DDNS 配置 56
5.5.1 申请 DDNS 帐号 56
5.5.2 配置 DDNS 服务 57
5.5.3 DDNS 验证 57

第 6 章 高级配置 59

6.1 端口映射和虚拟服务器 59
6.1.1 NAT 功能介绍 59
6.1.1.1 NAT 简介 59
6.1.1.2 NAT 地址空间 59
6.1.1.3 端口映射和虚拟服务器（DMZ 主机） 59
6.1.1.4 对称 NAT 60
6.1.1.5 端口映射配置 60
6.1.1.6 端口映射列表 61
6.1.1.7 自定义端口映射 61
6.1.1.8 端口映射配置实例 61
6.1.2 虚拟服务器配置 62
6.1.3 对称 NAT 62
6.2 路由配置 63
6.2.1 静态路由概述 63
6.2.2 系统保留路由 63
6.2.3 静态路由配置 65
6.2.4 路由信息列表 66
6.2.5 自定义静态路由 67
6.3 IP/MAC 绑定 69
6.3.1 IP/MAC 绑定功能介绍 69
6.3.1.1 IP/MAC 绑定概述 69
6.3.1.2 IP/MAC 绑定的工作原理 69
6.3.2 IP 和 MAC 绑定配置 71
6.3.3 IP/MAC 绑定全局配置 72
6.3.4 IP/MAC 绑定信息列表 73
6.3.5 自定义 IP/MAC 绑定条目 73
6.3.6 配置上网“白名单”和“黑名单” 74
6.3.6.1 配置上网“白名单” 74

6.3.6.2 配置上网“黑名单” 75
6.4 UPnP 配置 78
6.4.1 启用 UPnP 78
6.4.2 UPnP NAT 映射列表 78
6.5 即插即用 80
6.5.1 即插即用概述 80
6.5.2 即插即用配置 80
第 7 章 PPPOE 服务器 81
7.1 PPPoE 简介 81
7.1.1 PPPoE 连接 81
7.1.2 Discovery 阶段 81
7.1.3 PPP 会话阶段 82
7.1.4 PPPoE 连接的断开 82
7.2 PPPoE 服务器配置 83
7.2.1 PPPoE 服务器全局配置 83
7.2.2 账号配置 84
7.2.3 PPPoE 用户状态信息列表 84
7.3 PPPoE 服务器典型配置实例 85
第 8 章 带宽管理 87
8.1 带宽管理 87
8.1.1 带宽限速规则配置 87
8.1.2 用户带宽使用列表 88
8.1.3 带宽管理配置实例 88
8.2 地址组 90
8.2.1 地址组配置 90
8.3 时间段 92
8.3.1 时间段配置 92
8.3.2 时间段列表 94
8.3.3 自定义时间段 94
8.3.4 时间段配置实例 95
第 9 章 上网行为管理 98
9.1 上网行为管理 98
9.1.1 上网行为管理配置 98
9.1.2 上网行为管理列表 101
9.1.3 只允许 web 访问 102
9.1.4 上网行为管理配置实例 102
9.2 域名过滤 106
9.2.1 域名过滤配置 106
9.2.2 域名过滤全局配置 107
9.3 策略库 108
9.3.1 策略库概述 108
9.3.2 策略库信息列表 108

9.3.3 策略库版本检查 109
9.3.4 导入策略库 110

第 10 章 系统管理 111

10.1 管理员配置 111
10.2 时钟管理 112
10.3 软件升级 113
10.3.1 显示和保存当前运行软件 113
10.3.2 软件升级 113
10.4 配置管理 115
10.4.1 恢复出厂配置 115
10.4.2 重新启动设备 115
10.5 远程管理 117
10.6 系统信息 118
10.6.1 页面刷新功能 118
10.6.2 系统运行时间 118
10.6.3 系统资源状态 118
10.6.4 系统版本信息 119
10.6.5 系统端口状态 119

附录 A 配置局域网中的计算机 121

附录 B FAQ 124

1. ADSL 用户如何上网？ 124
2. 固定 IP 接入用户如何上网？ 125
3. 动态 IP（CABLE MODEM）接入用户如何上网？ 125
4. 如何将设备恢复到出厂配置? 126

附录 C 图索引 128

附录 D 表索引 131

导　　读

0.1　手册说明

本手册描述应用于 HiPER 500 系列产品在 ReOS 2009 软件平台的特性和功能，提供基于 WEB 界面的配置方法及其步骤。HiPER 500 系列各产品在功能和性能上有所不同，本手册中的部分功能如线路组合、策略库等均为 HiPER 520 产品所特有，用户应保证所使用的软件版本与本手册所描述对象一致。由于产品版本升级或其它原因，本手册内容会不定期更新。

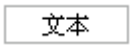
0.2　界面风格

WEB 管理界面遵循浏览器的习惯用法，如下所示：

单选框：选中代表只选用此项功能；

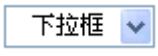
复选框：选中代表此选项所述功能被选中；

：单击则执行该按钮的动作；



：输入相关参数；

：通过列表框可以找到供选择的选项；



：通过下拉框可以找到供选择的选项。

0.3　基本约定

0.3.1　列表功能详解

WEB 界面中的列表有可编辑列表和只读列表两种类型，下面分别举例进行说明：

0.3.1.1 可编辑列表

可编辑列表用来显示、编辑各种配置信息，能够编辑、删除列表中的选项，此处以“端口映射列表”（如表 0-1）为例说明可编辑列表中各参数的含义。

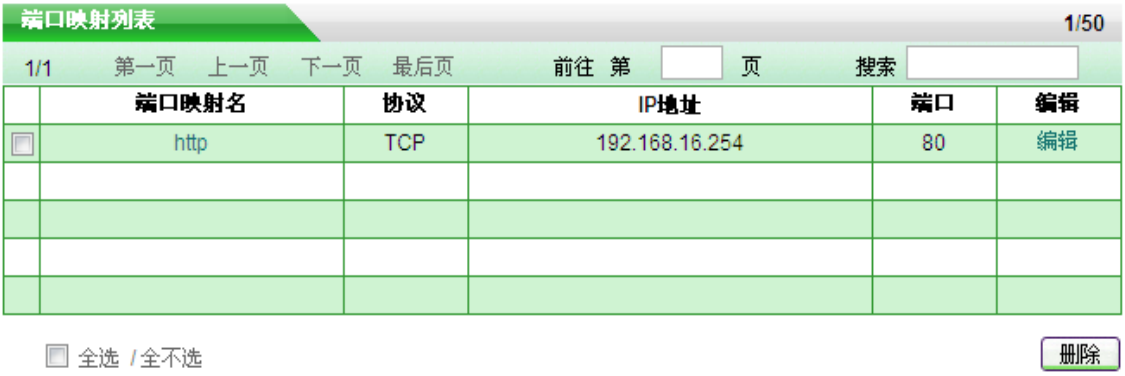


表 0-1 端口映射列表

1/1 ：当前页面序号/总页面数，此处指第 1 页/共 1 页；

第一页 ：超链接，单击即可转到第一页；

上一页 ：超链接，单击即可转到上一页；

下一页 ：超链接，单击即可转到下一页；

最后页 ：超链接，单击即可转到最后页；

前往 第 页 ：在文本框中输入页码，再敲<Enter>键或者单击“前往”，即可跳到指定页面；

搜索 ：在搜索文本框中输入要查询的字符串，再敲<Enter>键，即可显示所有与该字符串匹配的条目，并且，还可以在搜索结果中继续搜索。搜索完毕后，如果需要查看列表全部信息，则需在空的文本框中直接敲<Enter>键。

注意，如果一个条目有一个参数的值含有指定字符串（即子串匹配）时，就认为该条目与该字符串匹配。

1/50：当前已设置数目/最多可设置数目，此处指当前设置了 1 个端口映射条目，最多可设置 50 条端口映射；

编辑：超链接，单击即可进入相应编辑框；

全选 /全不选 ：选中后（方框中出现“√”），当前页面所有条目全部被选中；全选情况下，再单击该方框（方框变为空），当前页面所有条目全部未被选中；

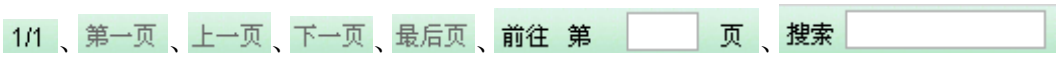
删除：先选择某条(或多条)需要删除的条目(单击其首列中的方框，方框中出现“√”，表示选中)，再单击“删除”按钮，即可删除选中的条目。

0.3.1.2 只读列表

只读列表用来显示系统状态信息，不可编辑，此处以“DHCP 地址使用信息列表”（如

表 0-2）为例说明只读列表中各参数的含义。

表 0-2 DHCP 地址使用信息列表



涵义均同前；

1/1：当前显示状态信息数/状态信息总数，此处指当前显示 DHCP 地址使用信息 1 条/共 1 条。

0.3.1.3 列表排序功能

设备中，WEB 界面的所有列表都支持排序功能。操作步骤如下：

在某个列表中，单击某列的标题，则按照该列数据对表中所有记录进行排序。第一次单击为降序，第二次单击为升序，第三次为降序，依次类推。每次排序后，列表重新从第一页开始显示。

0.3.2 符号约定

◆ 表示基本参数，描述参数基本涵义；

如果界面中某参数中有“*”号，表示该参数为必填项目。例如，如图 0-1 所示，“主 DNS 服务器”有“*”号，代表在配置 DNS 服务器时，该参数必须配置。

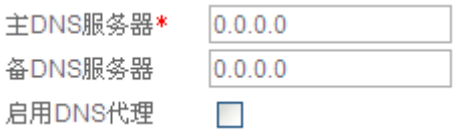


图 0-1 DNS 服务器配置

▶ 表示按钮，描述操作动作；

表示提示，指出重点注意事项。

0.3.3 键盘操作约定

<>：表示键盘上的按键。例如，<Enter>表示回车。

0.3.4 其他表达约定

1. 进入某配置界面的表达方式

一级菜单名称—>二级菜单名称（斜体加粗字体）用来表示打开某配置界面的路径。例如，*系统管理—>时钟管理*表示在 WEB 界面中，首先单击一级菜单“系统管理”，之后再单击二级菜单“时钟管理”，就进入时钟管理界面了。

2. 进行某动作的表达方式

单击“XXX”按钮（XXX 表示按钮名），表示进行该按钮所对应的操作。例如，单击“删除”按钮，就表示进行相应的删除操作，“删除”对应按钮

。

3. 选中某选项的表达方式

选中“XXX”选项（XXX 表示选项名），表示选中该选项所对应的功能。例如，选中“启用 DNS 代理”选项，就表示 DNS 代理功能被启用，如图 0-2 所示。

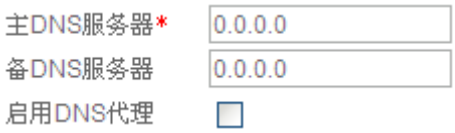


图 0-2 DNS 服务器配置

4. 常用动作按钮的涵义

下面将简要介绍 WEB 页面中几个常规按钮的作用，在手册其它地方不再说明。

：用于保存当前所做的配置；

：用于恢复到修改前的配置参数；

：用于刷新当前页面相关状态信息；

：用于删除列表中的选中的相关实例；

：用于获取相关功能的帮助信息。

0.4 出厂配置

1. 接口出厂配置如表 0-3 所示：

接口类型	IP 地址	子网掩码
LAN 口	192.168.16.1	255.255.255.0
WAN1 口	192.168.17.1	255.255.255.0
WAN2 口	192.168.18.1	255.255.255.0

表 0-3 接口出厂配置

2. 系统管理员的用户名出厂设置为“**Default**”（区分大小写），出厂密码为空。

0.5 内容简介

本手册主要介绍 HiPER 500 系列产品各功能的配置及应用，主要包括：产品概述、硬件安装、快速配置、快速向导、基本配置、高级配置、PPPoE 服务器、带宽管理、上网行为管理以及系统管理。

第 1 部分 产品概述

主要介绍 HiPER 500 系列产品的特点及功能特性。

第 2 部分 硬件安装

主要介绍 HiPER 500 系列产品的安装步骤及注意事项。

第 3 部分 快速配置

主要介绍了如何快速配置上网线路及一些必要的上网防范措施。通过导航条“开始菜单”可以快速接入下列页面进行相关配置：

- 线路配置上网（推荐）——点击即进入***基本配置—>线路配置***页面，进行上网线路配置；
- 不可不防（推荐）——点击即进入***基本配置—>安全专用配置***页面，进行必要的上网安全防范配置；
- 端口映射——点击即进入***高级配置—>端口映射和虚拟服务器***页面，进行端口映射和虚拟服务器；
- 系统信息——点击即进入***系统管理—>系统信息***页面，可以在该页面查看系统的各种信息；

第 4 部分 快速向导

主要介绍如何快速安装设备，包括：

- 上网接入线路配置——快速配置上网默认线路，设备提供 PPPoE、动态 IP、固定 IP 三种接入方式。

第 5 部分 基本配置

主要介绍产品的基本功能，包括：

- 线路配置——配置上网线路，查看线路连接信息；
- 线路组合——配置线路组合方式，设置线路组合相关参数。线路组合 HiPER 510 不提供；
- DHCP 和 DNS 服务器——配置 DHCP 服务器及 DNS 服务器，查看 DHCP 地址使用信息；
- 接口配置——配置设备物理接口的相关参数；

- DDNS 服务——申请、配置 DDNS 服务；

第 6 部分 高级配置

主要介绍产品的高级功能配置，包括：

- 端口映射和虚拟服务器——配置虚拟服务器、端口映射，查看端口映射列表；
- 路由配置——配置静态路由，预先指定对某一网络访问时所要经过的路径；
- IP/MAC 绑定——配置 IP/MAC 绑定用户，防止 IP 地址盗用，配置上网“黑名单”和“白名单”；
- UPnP——启用 UPnP 服务，查看通过 UPnP 建立起来的端口映射信息；
- 即插即用——为网络的内网用户提供不修改原有地址即能上网的功能；

第 7 部分 PPPoE 服务器

主要介绍产品的 PPPoE 服务器的功能配置，包括 PPPoE 账号的配置以及配置 PPPoE 服务器的全局参数，并可查看配置的 PPPoE 账号信息。

第 8 部分 带宽管理

主要介绍带宽管理的相关功能，包括：

- 带宽管理——配置基于地址组的限速规则，有效管理网络带宽；并可查看在线用户的带宽使用情况；
- 地址组——可将访问权限相同的多个不连续的 IP 地址段或地址组划分到一个地址组内，然后为该地址组配置相关的策略；
- 时间段——配置时间段实例；

第 9 部分 上网行为管理

主要介绍上网行为管理的相关功能，包括：

- 上网行为管理：提供配置局域网用户上网行为的管理和控制，提高内网带宽使用和网络安全；
- 域名过滤——允许或禁止内网用户访问某些指定的域名；

第 10 部分 系统管理

主要介绍产品相关管理参数的设置，包括：

- 管理员配置——设置 WEB 管理员密码；
- 时钟管理——手工或自动设置系统时间和日期；
- 软件升级——升级当前软件版本，下载最新软件升级；
- 配置管理——恢复设备出厂配置；
- 远程管理——配置远程管理，允许或禁止远程 HTTP 服务。

第 11 部分 附录

本手册共提供 4 个附录，描述如下：

- 附录 A 配置局域网中计算机——提供配置局域网计算机的 TCP/IP 属性的方法。
- 附录 B FAQ——提供常见问题解答；
- 附录 C 图索引——提供本手册所有图的索引目录；
- 附录 D 表索引——提供本手册所有表的索引目录。

第1章 产品概述

非常感谢您选用上海艾泰科技有限公司的 HiPER 500 系列产品！

本章主要讲述 HiPER 500 系列产品的功能和特点。

1.1 关键特性

- 共享 Internet 接入（ADSL、Cable Modem、以太网接入）
- 支持 DHCP 服务器和客户端功能
- 支持静态路由
- 支持端口映射，支持 DMZ 主机
- 支持对内网用户进行上网行为管理，可对常用的即时通讯软件（QQ、MSN 和飞信等）、P2P 软件（BT 软件，PPLive 等）、热门游戏（QQ 游戏、魔兽世界等游戏）等软件进行管制
- 功能丰富的 PPPoE 服务器功能
- 防止 DoS/DDoS 攻击
- 支持 DNS 请求过滤
- 支持 DDNS
- 支持网络时间同步
- 支持 UPnP
- 支持 MAC 地址克隆
- 支持时间段管理
- 支持地址组管理
- 支持带宽管理功能，可根据 IP 地址限制带宽
- 支持 IP/MAC 绑定，可设置上网黑名单和白名单；还支持 IP/MAC 全部绑定和自动绑定功能，配置更加简单智能
- 提供基于 WEB UI 和命令行（CLI）的配置界面，支持远程管理
- 支持 WEB、TFTP 多种升级方式，方便功能扩展

1.2 主要特点

1. 局域网接口（LAN）

- 多端口交换机：集成了多端口 10/100Mbps 自适应交换机（MDI/MDI-X 自适应）。
- 支持 DHCP Server：支持 DHCP Server 功能，给局域网中的计算机动态分配 IP 地址以及网关、DNS Server 等信息。

2. 广域网接口（WAN）

- WAN 口：提供 10/100M 自适应广域网接口（MDI/MDI-X 自适应）。
- 支持 DSL 或者 Cable Modem：HIPER 500 系列通过了市场上众多厂商的 DSL Modem 和 Cable Modem 的兼容性测试。
- 支持 PPPoE：广域网接口支持使用 PPPoE（PPP over Ethernet）协议和 ISP 连接。
- 共享 Internet 访问：局域网的所有用户可以通过 NAT（Network Address Translation）共享多条 Internet 线路上网。

3. IP/MAC 绑定和业务控制

- 支持 IP 地址和 MAC 地址绑定。
- 支持多种 Internet 业务的管理与控制。

4. IP QoS 功能

- 基于地址组的个性带宽管理功能，实现对内网主机上传/下载速率的控制，有效控制内网传输速率，提高带宽利用率。

5. 配置和管理

- 简易配置：基于 Web UI 或者命令行（CLI）的配置界面，方便管理和配置。
- 开始菜单：提供常用页面导航功能，可快速地配置线路上网、基本的病毒防御等。
- 远程管理：在局域网或者广域网上的任何一台计算机上均可实现对设备的远程管理。
- 重启设备：可在任何页面对设备进行重启，方便用户操作。

6. Internet 高级特性

- 虚拟服务器（DMZ 主机）：支持配置 DMZ 主机，DMZ 主机将完全暴露在 Internet 上，方便远程用户访问。
- 端口映射：支持用户自定义多条端口映射，方便远程用户访问内部服务器的指定服务端口。
- DDNS：支持动态域名服务。
- PPPoE 服务器：支持 PPPoE 服务器功能，并提供丰富的设置。

7. 安全特性

- 密码管理：设置管理员口令，可以防止未被授权的用户修改设备的配置。
- 上网行为管理：可以设置禁止内网用户进行 QQ/MSN/BT 下载，禁止讯雷搜索资源，禁止使用网络游戏，禁止使用 HTTP 下载扩展名为 exe、dll、vbs、com、bat、sys 的文件，禁止用户在网页上提交输入，禁止访问股票网站，禁止访问游戏网站，禁止使用 HTTP 代理等功能。

1.3 规格

- 符合 IEEE802.3Ethernet 以及 IEEE802.3u Fast Ethernet 标准。
- 支持 TCP/IP、PPPoE、DHCP、ICMP、NAT、静态路由等协议。
- 各个物理端口均支持自动协商功能，自动调整传输方式和传输速度。
- 各个物理端口均支持 MDI/MDI-X 正反线自适应。
- 提供状态指示灯。
- 工作环境：温度：0-40℃

  高度：0-4000m

  相对湿度：10-90%，不结露

第2章 硬件安装

本章主要讲述如何安装 HiPER 500 系列产品及注意事项。

2.1 安装准备

1. 以太网和 TCP/IP 协议。
2. 准备 DSL 或者 Cable Modem，并从 ISP 那里获得访问 Internet 的用户名和密码。

2.2 安装流程

在安装设备之前，必须保证设备的电源是关闭的。HIPER 500 系列产品的安装流程一般经过以下几个步骤：

第一步，选择安装地点，一般是将设备安装在工作台上。

第二步，建立设备与局域网的连接，即将管理计算机或交换机连接到设备的局域网端口。

第三步，建立设备与广域网的连接，即将 Cable/DSL Modem 连接到设备的广域网端口。

第四步，打开电源，打开电源之前确保电源供电、连接、接地正常。

第五步，检查系统指示灯，查看设备的连接及工作状态是否正常。

以下各节将分别介绍产品的安装步骤、接线图及指示灯状态。

2.3 安装步骤

2.3.1 HiPER510 安装步骤

1. 选择安装地点

选择一个适当的地方安装 HiPER 510，确保设备和 Cable/DSL Modem 的电源是关闭的，一般将设备放置在干净的工作台上。

注意：请保证工作台的平稳性和良好接地，同时不要在设备上面放置重物。

2. 连接设备到管理计算机或局域网

使用标准的网线连接管理计算机到设备的局域网（LAN）口，或者是连接交换机到设备的 LAN 口，如图 2-1 所示。HiPER 510 将会自动适应 10M 或者是 100M 的设备。

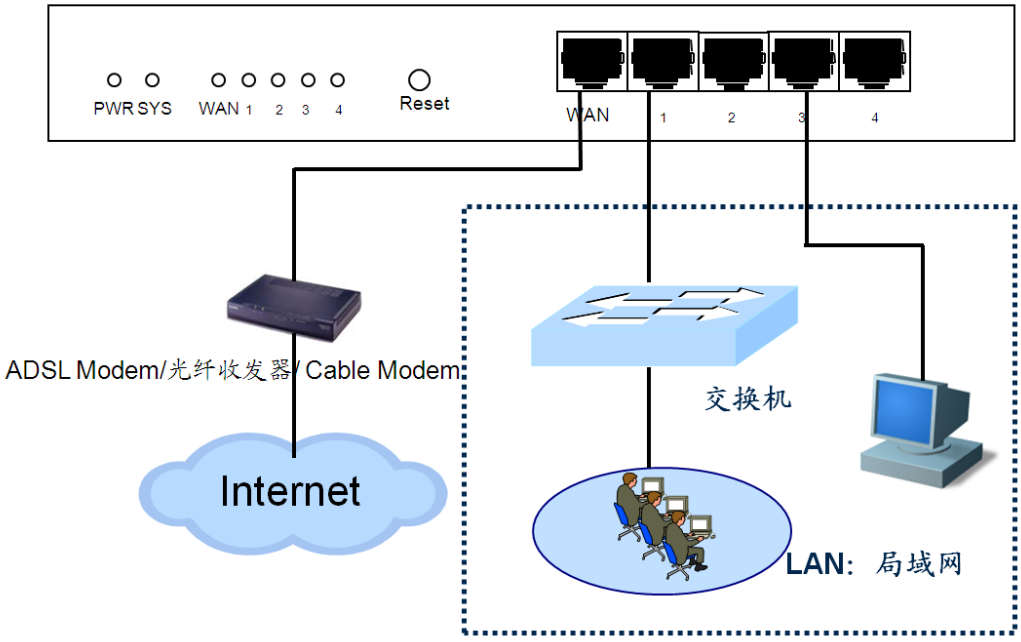


图 2-1 建立局域网和广域网连接——HiPER 510

3. 连接设备到 Internet

使用 Cable/DSL Modem 厂商提供的网线将 Cable/DSL Modem 连接到 HiPER 510 的广域网（WAN）口，如图 2-1 所示。如果没有厂商提供的网线，请使用标准网线。

4. 打开电源

将随机配置的电源线连接到 HiPER 510 后面板的电源接口。

注意！连接电源之前确保电源供电、连接、接地正常，否则可能造成系统工作异常或系

统损坏。

5. **检查系统指示灯**

系统指示灯位于前面板左方，分为 2 组（如图 2-2）：第一组是左边的 1 行 2 列，共 2 个，状态如表 2-1 所示；第二组是右边的 1 行 5 列，共 5 个，1-4 对应 LAN 口的四个交换口，WAN 对应 WAN 口，具体状态如表 2-2 所示。

图 2-2 系统指示灯——HiPER 510

指示灯	启动时状态	启动后状态
PWR	常亮	电源工作正常时常亮
SYS	启动 1 秒后，先快速闪烁 1 秒，熄灭 2 秒后开始以每秒 2 次的频率闪烁	以每秒 2 次的频率闪烁，系统负担较大时，闪烁频率降低；有故障时常亮或常灭。

表 2-1 第一组指示灯

指示灯	启动时状态	启动后状态
1,2,3,4 WAN	闪烁后熄灭	当有设备连接到相应端口，100M 协商成功，该端口对应指示灯常亮，有流量时闪烁。

表 2-2 第二组指示灯

2. Reset 按钮

Reset 按钮指复位按钮，在忘记管理员口令时可以通过此按钮来恢复设备的出厂配置。操作方法为：在带电运行过程中，按住 Reset 按钮 5 秒钟以上，再松开此按钮，设备将恢复到出厂配置，并自动重启。

2.3.2 HiPER520 安装步骤

1. **选择安装地点**

选择一个适当的地方安装 HiPER 520，确保设备和 Cable/DSL Modem 的电源是关闭的，一般将设备放置在干净的工作台上。

注意：请保证工作台的平稳性和良好接地，同时不要在设备上面放置重物。

2. **连接设备到管理计算机或局域网**

使用标准的网线连接管理计算机到设备的局域网（LAN）口，或者是连接交换机到设备的 LAN 口，如图 2-3 所示。HiPER 520 将会自动适应 10M 或者是 100M 的设备。

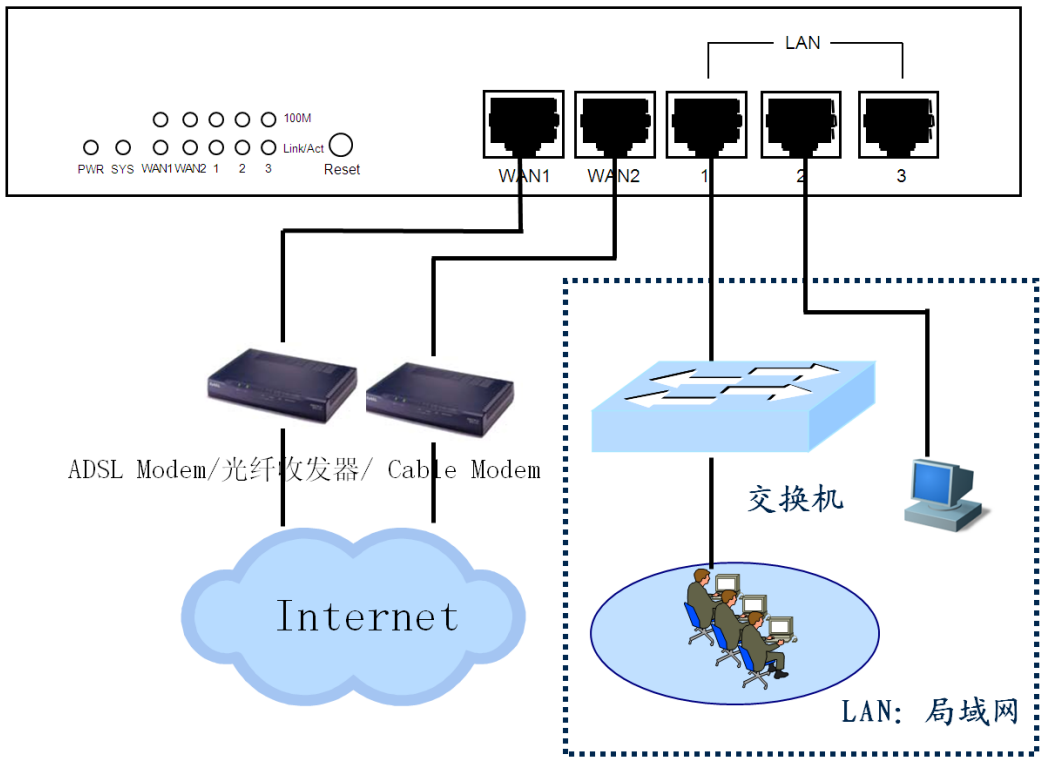


图 2-3 建立局域网和广域网连接——HiPER 520

3. 连接设备到 Internet

使用 Cable/DSL Modem 厂商提供的网线将 Cable/DSL Modem 连接到 HiPER 520 的广域网（WAN）口，如图 2-3 所示。如果没有厂商提供的网线，请使用标准网线。

4. 打开电源

将随机配置的电源线连接到 HiPER 520 后面板的电源接口。

注意！连接电源之前确保电源供电、连接、接地正常，否则可能造成系统工作异常或系统损坏。

5. 检查系统指示灯

系统指示灯位于前面板左方，分为 2 组（如图 2-4）：第一组是左边的 1 行 2 列，共 2 个，状态如表 2-3 所示；第二组是右边的 1 行 5 列，共 5 个，1-4 对应 LAN 口的四个交换口，WAN 对应 WAN 口，具体状态如表 2-4 所示。

图 2-4 系统指示灯——HiPER 520

指示灯	启动时状态	启动后状态
PWR	常亮	电源工作正常时常亮

SYS	启动 1 秒后，先快速闪烁 1 秒，熄灭 2 秒后开始以每秒 2 次的频率闪烁	以每秒 2 次的频率闪烁，系统负担较大时，闪烁频率降低；有故障时常亮或常灭。

表 2-3 第一组指示灯

指示灯	启动时状态	启动后状态
100Mbps	闪烁后熄灭	当有设备连接到相应端口，100M 协商成功，该端口对应指示灯常亮，有流量时闪烁。
Link/Ackt	闪烁后熄灭	当有设备连接到相应端口，协商成功，该端口对应指示灯长亮，该端口有网络流量时闪烁。

表 2-4 第二组指示灯

3. Reset 按钮

Reset 按钮指复位按钮，在忘记管理员口令时可以通过此按钮来恢复设备的出厂配置。操作方法为：在带电运行过程中，按住 Reset 按钮 5 秒钟以上，再松开此按钮，设备将恢复到出厂配置，并自动重启。

第3章 快速配置

本章主要介绍如何为管理计算机配置正确的网络设置、如何使用*开始*菜单快速地配置上网所需要的基本参数、必要的安全防范措施等以及如何使用快捷图标快速链接到艾泰科技有限公司网站获得产品信息和服务。

3.1 配置正确的网络设置

在通过 WEB 界面登陆到设备之前，首先要对管理计算机进行正确的网络设置。

首先将计算机连接到设备的某个局域网端口，接下来设置计算机的 IP 地址。

第一步，设置计算机的 TCP/IP 协议，请参考附录 A。如果已经正确设置完成，请跳过此步。

第二步，设置计算机的 IP 地址为 192.168.16.2-192.168.16.254 中的任意一个地址，子网掩码为 255.255.255.0，默认网关为 192.168.16.1（设备的 LAN 口 IP 地址），DNS 服务器为当地运营商提供的地址。

第三步，使用 Ping 命令检查计算机和设备之间是否连通。下面的例子是在 Windows XP 环境中，执行 Ping 命令：**Ping 192.168.16.1**

如果屏幕显示如下，表示计算机已经成功和设备建立连接。

```
Pinging 192.168.16.1 with 32 bytes of data:

Reply from 192.168.16.1: bytes=32 time<1ms TTL=255
Reply from 192.168.16.1: bytes=32 time<1ms TTL=255
Reply from 192.168.16.1: bytes=32 time<1ms TTL=255
Reply from 192.168.16.1: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.16.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
```

如果屏幕显示如下，表示计算机和设备连接失败。

```
Pinging 192.168.16.1 with 32 bytes of data:

Request timed out.

Request timed out.

Request timed out.

Request timed out.

Ping statistics for 192.168.16.1:
```

连接失败时，请做以下检查：

1. 硬件连接：设备面板上与该局域网端口对应的 Link/Act 指示灯和计算机上的网卡灯必须亮。

2. 计算机 TCP/IP 属性的配置：如果设备的 IP 地址为 192.168.16.1，那么计算机的 IP 地址必须为 192.168.16.2-192.168.16.254 中的任意一个空闲地址，即计算机的 IP 地址必须和设备的 LAN 口地址在同一个 IP 子网内。

3.2 开始菜单

*开始*菜单位于 WEB 界面的一级菜单栏的最左边，它提供了快速进入其他页面的接口，通过*开始*菜单，用户可以快速地配置上网所需要的基本参数、必要的安全防范措施及查看路由器的相关状态信息等。

3.2.1 登录设备

计算机如果是使用 MS Windows、Macintosh、Unix 或者是 Linux 等任何操作系统，都可以通过浏览器（Internet Explorer 或 Netscape Communicator）来对设备进行配置。

打开浏览器，在浏览器的地址栏里输入设备的 IP 地址，例如 192.168.16.1，如图 3-1 所示。

连接建立起来之后，将会看到如图 3-1 所示的登录界面。首次使用时需要以系统管理员的身份登录，即在该登录界面输入系统管理员的用户名和密码（用户名的出厂设置为“Default”，密码的出厂设置为空），然后单击“确定”按钮。

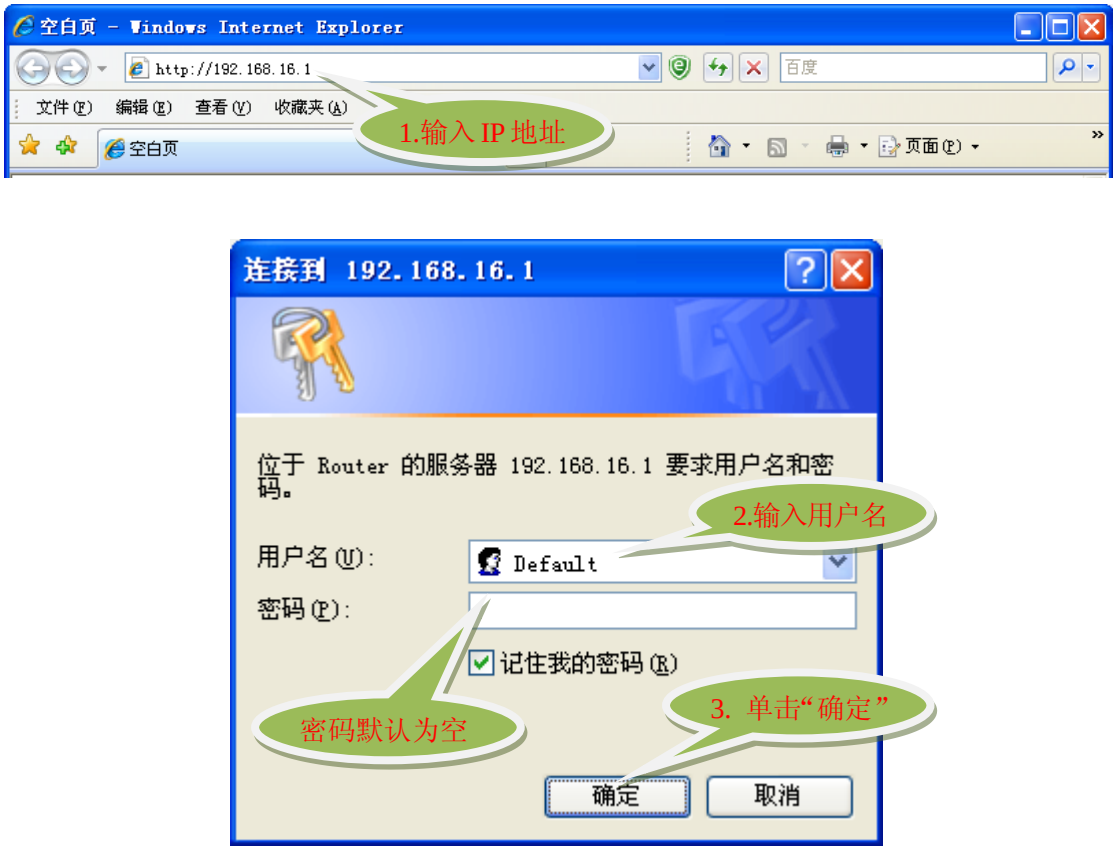


图 3-1 WEB 登录界面

如果用户名和密码正确，浏览器将显示管理员模式的首页，该页面右上角显示系统型号及版本信息。在首页中，针对每个一级菜单，都提供一个图标，单击某个图标即可进入相关

页面。

若用户还没配置任何上网线路，系统右下角将显示提示信息“欢迎使用艾泰产品！如果您是第一次登录，请单击“快速向导”完成配置！”，如下图所示。

图 3-2 WEB 界面首页

图 3-3 开始菜单的子菜单

单击“开始”，开始菜单下即显示线路配置上网、不可不防、端口映射、和系统信息 4 个子菜单（如上图所示），通过这些子菜单可以进行快速上网配置。单击各子菜单，即可进入各子菜单对应的页面进行相应的配置。

3.2.2 线路配置上网

单击***线路配置上网***，则转到***基本配置—>线路配置***页面，在该页面不仅可以配置线路，也可以根据实际需要修改或删除已配置的线路，还可以查看各条线路的连接状态信息（具体的配置方法及各参数的涵义见***基本配置—>线路配置***<章节 5.1>，这里不重复介绍）。

只有在配置完“默认线路”之后，才能配置其他上网线路。当配置完默认线路后，系统会提示用户是否进入“不可不防”，单击“确定”按钮，进入不可不防页面进行安全防御配置；如果你还需要配置其他上网线路，单击“取消”按钮，返回到线路配置页面，继续配置

其他线路（如图 3-4 所示）。

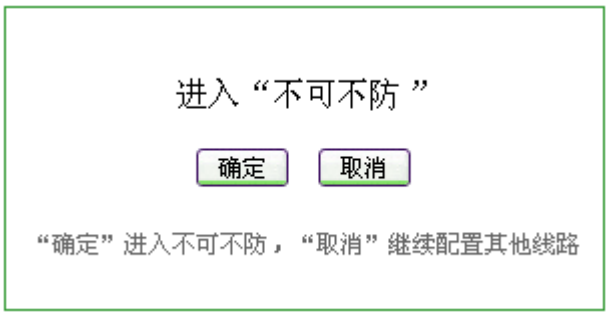


图 3-4 提示信息

3.2.3 不可不防

该页面提供双线路路由配置及上网必要的安全防范措施，包括 ARP 欺骗防御、冲击波病毒防御等。

如果用户未配置任何线路而直接进入本页面，系统会提示“请先配置默认线路”，单击“确定”，跳转到***基本配置—>线路配置***页面进行上网线路配置。

3.2.3.1 双线路路由配置

在本页面可以进行双线路路由配置，用户可以通过“WAN1 口/WAN2 口运营商选择”选择相应的运营商，系统将根据用户的选择生成相对应的路由，比如电信生成电信路由，网通生成网通路由。

通过 WAN1 口/WAN2 口运营商选择，可以方便地实现电信流量走电信线路，网通流量走网通线路，如图 3-5 所示。

图 3-5 双线路路由配置

- WAN1 口运营商选择：选择 WAN1 口运营商，有三个可选项分别为电信线路、网通线路及其他线路，此处选择电信线路，表示电信流量走 WAN1 口；
- WAN2 口运营商选择：选择 WAN2 口运营商，有三个可选项分别为电信线路、网通线路及其他线路，此处选择网通线路，表示网通流量走 WAN2 口。

提示：

双线路路由配置只支持 WAN1 口和 WAN2 口，如果您配置了其他 WAN 口的多线路连接，该页面不会出现线路组合配置的相关参数。

3.2.3.2 病毒防御

本页面提供基本的网络安全防御配置，用来提升网络的安全性。通过在本页面进行简单地配置，可以有效防御 ARP 欺骗、DoS/DDoS 攻击、冲击波以及震荡波等常见病毒攻击，为用户提供一个健壮、安全的网络环境。

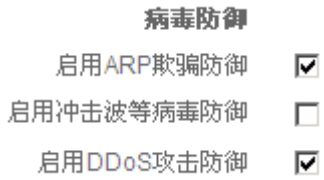


图 3-6 病毒防御

- 启用 ARP 欺骗防御：打勾表示启用，启用后，并将局域网所有 PC 的 IP/MAC 地址对全部绑定，设备就可以有效防御内网 ARP 欺骗攻击了；
- 启用冲击波等病毒防御：打勾表示启用，启用后， 设备 将有效防御冲击波、震荡波等常见病毒攻击。启用此功能后，设备将直接丢弃 LAN 口接收到的协议为 TCP，目的端口为 135、136、137、138、139、445、1025、5554、9996 的数据包，此时，局域网主机将无法访问外网主机提供的相关端口服务，例如 windows 文件共享服务、打印共享服务等；
- 启用 DDoS 攻击防御：打勾表示启用，启用后，设备 将有效防御内网常见的 DoS/DDoS 攻击。目前，只能防御伪造源地址攻击。启用此功能后，设备将只允许源 IP 地址与 LAN 口 IP 地址在同一个网段的数据包通过，此时，三层交换机后的主机将不能通过设备访问外网。

3.2.4 端口映射

单击*开始—>端口映射*即可转到*高级配置—>端口映射和虚拟服务器*（章节 6.1）页面，在该页面可以进行端口映射和虚拟服务器配置，还可以在“端口映射列表”中查看已配置的相关信息。

提示：具体的配置方法及参数解释请参见章节“6.1 端口映射和虚拟服务器”，这里不再重复描述。

3.2.5 系统信息

单击*开始—>系统信息*，即可转到*系统信息*页面，在该页面管理员可以查看系统运行时间、版本及资源状态以及端口状态等。

3.2.5.1 页面刷新功能

图 3-7 页面刷新功能配置

- 下拉框：用于设置采用手动或自动刷新本页面及相关页面。

  手动刷新：表示不启用自动刷新功能，只能通过单击“刷新”按钮手动刷新本页面；

  自动刷新/10 秒、自动刷新/30 秒或者自动刷新/60 秒：表示启用自动刷新功能，本页面将每隔指定的时间间隔自动刷新。

- 刷新：单击“刷新”按钮，可查看本页面最新信息。

提示：若修改了下拉框的值，只有在单击“刷新”按钮之后，修改的配置才能被保存并生效。

3.2.5.2 系统运行时间

图 3-8 系统运行时间

- 系统时间：显示设备当前的日期和时间；
- 系统运行时间：显示设备本次启动至查看时刻的时间。

3.2.5.3 系统资源状态

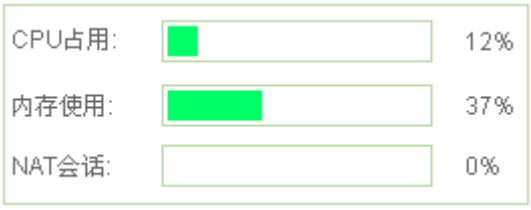


图 3-9 系统资源状态

- CPU 占用：显示当前 CPU 占用的百分比；
- 内存使用：显示当前内存使用的百分比；
- NAT 会话：显示当前建立的 NAT 会话数占设备所能处理的最大 NAT 会话数的百分比。

提示：

1. 上述三个参数的值都通过进度条和数值（百分比）两种方式显示，数值的取值范围为 0%~100%；根据数值的大小，进度条可能会显示为空、绿色、黄色或者红色：

- 当数值＜1%时，进度条为空；
- 当 1%≤数值＜50%时，进度条为绿色；
- 当 50%≤数值＜70%时，进度条为黄色；
- 当数值≥70%时，进度条为红色。

2. 上述三个参数显示了设备接近于满负荷运行的程度。如果它们的值都比较低，就表明设备还有能力处理比它现在所运行的更多的网络通讯。如果它们的值都很高，就表明设备已经接近于满负荷工作，此时再增加更多的任务可能会导致系统对通讯的处理出现延迟。

3.2.5.4 系统版本信息

图 3-10 系统版本信息

- 序列号：产品的内部序列号（和表面序列号可能不同）；
- 功能号：产品具有的功能模块；
- 软件版本：产品的软件版本号。

3.2.5.5 系统端口状态

端口	状态	外出/进入速率(kbit/s)
lan1	100M Full MDI-X	26 / 3
lan2	DOWN	
lan3	DOWN	
lan4	DOWN	

端口	状态	外出/进入速率(kbit/s)
wan1	100M Full MDI	2 / 53

表 3-1 系统的端口状态

- 端口：其中，上图中的 LAN 接口有 4 个交换端口；
- 状态：若某端口未激活，其“状态”显示为 DOWN；若已经激活，则依次显示该端口的工作速率、工作状态（Full-全双工，Half-半双工）以及工作模式（MDI-正接，MDI-X-反接）；
- 外出/进入速率（kbit/s）：相关速率是针对接口统计的，即 4 个交换端口按照 1 个 LAN 口来统计。

3.3 快捷图标

在 WEB 界面一级菜单栏的上面提供了“同类产品、软件下载、产品资料、产品注册、预约服务、产品讨论以及投诉建议”7 个快捷图标，用于快速链接到艾泰科技公司网站的相关页面。

图 3-11 快捷图标

这 7 个快捷图标的作用如下：

- 同类产品——链接到艾泰网站的产品中心页面，查找更多此类产品；
- 软件下载——链接到艾泰网站的下载中心页面，下载产品最新软件；
- 产品资料——链接到艾泰网站的下载中心页面，下载产品手册、产品速查等产品资料；
- 产品注册——链接到艾泰网站产品登记页面，注册您的产品信息；
- 预约服务——链接到艾泰网站预约服务页面，预约下一工作日的客户服务；
- 产品讨论——链接到艾泰网站 BBS 论坛，参与产品的讨论；
- 投诉建议——链接到艾泰网站投诉建议页面，反馈您在产品使用中遇到的问题和对产品的建议。

WEB 界面的每个功能页面均提供一个到网站知识库的超链接，单击超链接即可链接到艾泰科技公司网站的知识库，查找与本页功能相关的所有技术资料。

图 3-12 网站知识库超链接

提示：只有当路由器配置可以上网时，单击这些图标和超链接才能成功。

第4章 快速向导

通过阅读本章内容，可以设置设备上网所需的基本网络参数，快速地将设备连接到Internet。如果已经通过开始菜单配置了上网线路，在该页面就无需再配置上网线路。

在进入快速向导配置“上网默认线路”之前，应正确配置局域网中计算机的网络设置，具体方法见“章节 3.1 配置正确的网络设置”。

4.1 快速向导

进入设备 WEB 首页“快速向导”设置界面。快速向导提供配置设备的默认线路接入配置。

4.1.1 上网接入方式设置

快速向导的第一页配置页面还可以对上网接入方式进行设置，设备支持以下三种常用的上网方式，可以根据实际情况进行选择。

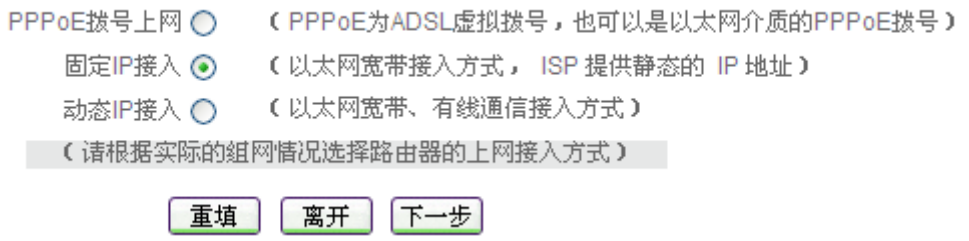


图 4-1 上网接入方式设置

- PPPoE 拨号上网：ADSL 虚拟拨号（也可以是以太网介质的 PPPoE 拨号）；
- 固定 IP 接入：以太网宽带接入方式，ISP（例如中国电信）提供静态的 IP 地址；
- 动态 IP 接入：以太网宽带或者有线通信接入方式，ISP（例如中国电信）通过 DHCP 服务为用户分配 IP 地址。
- 重填：恢复到修改前的默认线路接入方式；
- 离开：离开快速向导页面，进入主页面，快速向导所有操作无效；
- 选中“PPPoE 拨号上网”选项，单击“下一步”按钮，即可进入快速向导的第二页 PPPoE 拨号页面；
- 选中“固定 IP 接入”选项，单击“下一步”按钮，即可进入快速向导的第二页固定 IP 接入页面；
- 选中“动态 IP 接入”选项，单击“下一步”按钮，即可进入快速向导的第二页动态 IP 接入页面。

4.1.2 上网接入线路配置

4.1.2.1 上网接入线路配置的注意事项

1. 通过快速向导配置的上网线路的名称缺省为“默认线路”，并且，它固定连接到设备的 WAN1 接口；可以在***基本配置—>线路配置***的“线路连接信息列表”中，查看“默认线路”的配置和状态信息。

2. 如果改变了设备的“局域网 IP 地址”，系统会出现对话框显示“局域网 IP 地址已变为 xxxx”，“xxxx”为更改后的 IP 地址，在完成本向导之后，必须使用新的 IP 地址重新登录设备，才能进行 WEB 界面管理；并且，局域网中所有计算机的默认网关必须设置成该 IP 地址才能正常上网。

3. 如果发现完成配置后不能上网，请检查各项配置是否正确；也可以直接到***基本配置—>线路配置***中检查线路状态，查看、修改配置参数。

4.1.2.2 PPPoE 拨号上网配置

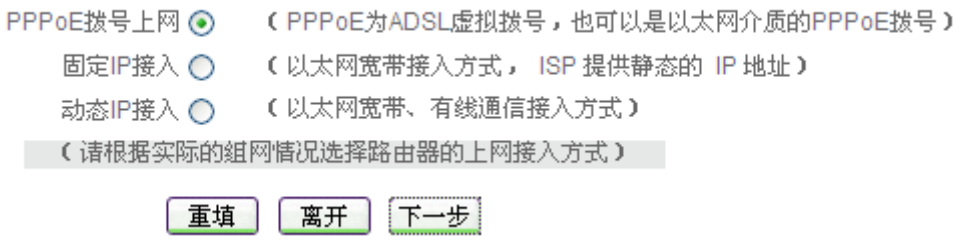


图 4-2 PPPoE 拨号上网方式

在选择上网接入方式页面中，选中“PPPoE 拨号上网”选项，如图 4-2 所示。单击“下一步”按钮，进入 PPPoE 配置页面（如图 4-3），配置 PPPoE 信息，单击“完成”按钮，PPPoE 拨号上网线路配置完成，同时，系统密码、系统日期和系统时间也成功修改。

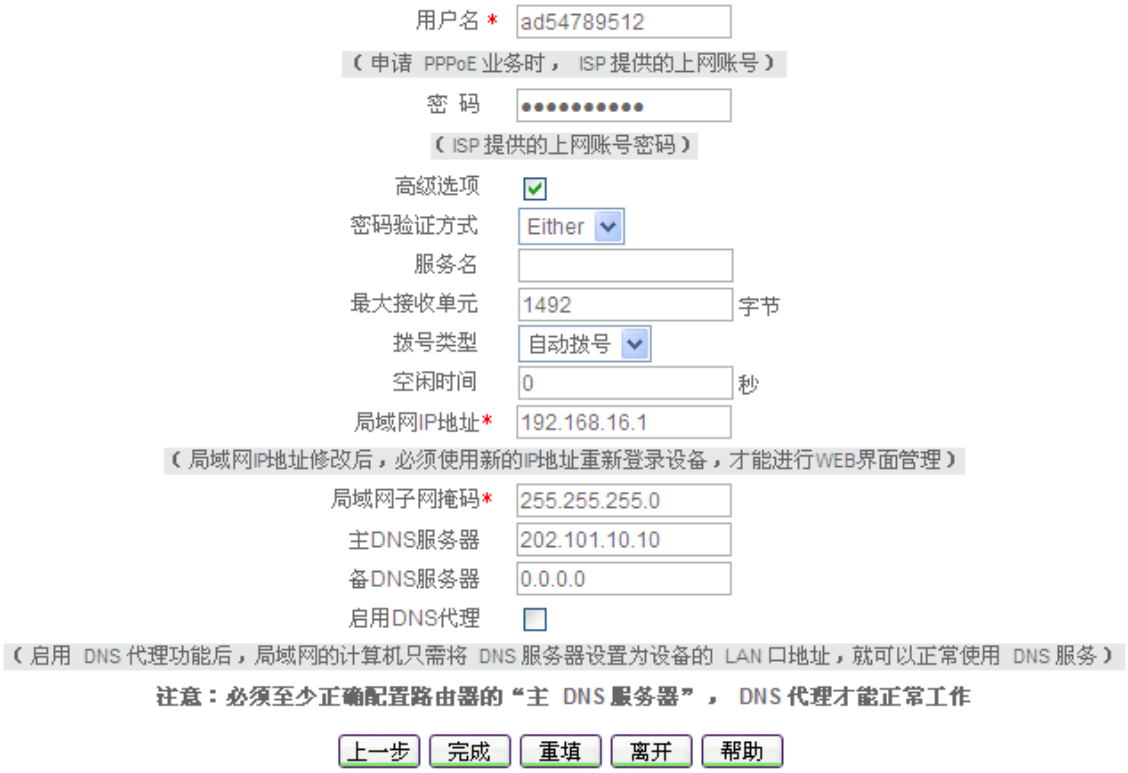


图 4-3 PPPoE 拨号配置

- 用户名、密码：申请 PPPoE 业务的时候，ISP（例如中国电信）将提供上网账号及密码（如有疑问，请询问 ISP）；
- 密码验证方式：ISP 验证用户名及密码的方式，多数地区为 PAP 方式，也有少数地区采用 CHAP 方式，NONE 表示不进行用户名和密码验证，Either 表示自动和对方设备协商采用哪种验证方式（如有疑问，请询问 ISP）；
- 局域网 IP 地址、子网掩码：配置成功后，该地址将作为局域网中计算机用作上网的网关地址（出厂值为 192.168.16.1/255.255.255.0）；
- 服务名：ISP 提供的 PPPoE 服务名，一般不需要设置（如有疑问，请询问 ISP）；
- 最大接收单元：缺省值为 1492 字节，PPPoE 拨号时设备将自动与对方设备协商，除非特别应用，不要修改；
- 拨号类型：

  自动拨号：当开启设备或者上一次拨号断线后自动拨号连接；

  手动拨号：在***基本配置—>线路配置***的“线路连接信息列表”中手动进行连接和挂断；

  按需拨号：在局域网内部有访问 Internet 流量时设备自动进行连接；
- 空闲时间：在没有访问 Internet 流量后自动断线前等待的时长，0 代表不自动断线（单位：秒）；
- 主 DNS 服务器：ISP（例如中国电信）提供的主用 DNS 服务器的 IP 地址，可不配置，线路连接成功后，设备将自动从 ISP 处获得；
- 备 DNS 服务器：ISP（例如中国电信）提供的备用 DNS 服务器的 IP 地址。
- 启用 DNS 代理：选中之后，设备会启用 DNS 代理功能，此时给局域网中的计算机

分配的主 DNS 服务器的 IP 地址就是设备局域网接口的 IP 地址。

- 上一步：返回到快速向导的第一页；
- 重填：恢复到修改前的 PPPoE 配置参数；
- 离开：离开快速向导页面，进入主页面，快速向导所有操作无效；
- 完成：快速向导运行成功，所做的操作在这里生效。

提示：所做的操作，只有单击“完成”按钮才生效（包括快速向导的前一页）。

4.1.2.3 固定 IP 接入配置

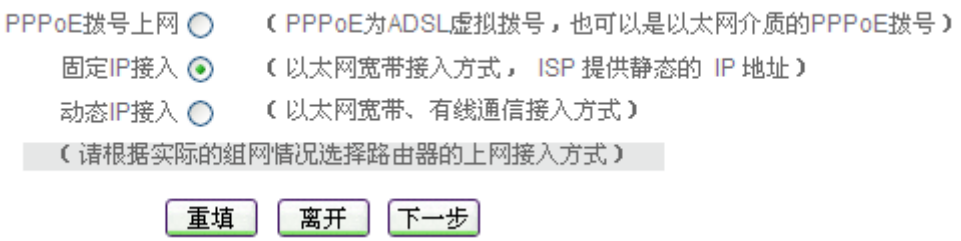


图 4-4 固定 IP 接入方式

在选择上网接入方式页面中，选中“固定 IP 接入”选项，如图 4-4 所示。单击“下一步”按钮，进入固定 IP 接入页面（如图 4-5，在这里配置固定 IP 接入信息，单击“完成”按钮，固定 IP 接入线路配置完成，同时，系统密码、系统日期和系统时间也成功修改。

图 4-5 固定 IP 接入配置

- 局域网 IP 地址、子网掩码：配置成功后，该地址将作为局域网中计算机用作上网的网关地址（出厂值为 192.168.16.1/255.255.255.0）；
- 广域网 IP 地址、子网掩码、静态网关：申请固定 IP 接入业务的时候，ISP（例如中国电信）将提供设备使用的广域网 IP 地址、子网掩码和静态网关；
- 主 DNS 服务器：ISP（例如中国电信）提供的主用 DNS 服务器 IP 地址；
- 备 DNS 服务器：ISP（例如中国电信）提供的备用 DNS 服务器 IP 地址；
- 启用 DNS 代理：选中之后，设备会启用 DNS 代理功能，此时给局域网中的计算机

分配的主 DNS 服务器的 IP 地址就是设备局域网接口的 IP 地址。

- 上一步：返回到快速向导的第一页；
- 重填：恢复到修改前的固定 IP 配置参数；
- 离开：离开快速向导页面，进入主页面，快速向导所有操作无效；
- 完成：快速向导运行成功，所做的操作在这里生效。

提示：

1. 所做的操作，只有单击“完成”按钮才生效（包括快速向导的前几页）；

2. 广域网 IP 地址、静态网关要在同一网段，某些 ISP（例如中国电信）提供的广域网 IP 地址和静态网关不在同一网段，请修改子网掩码，使它们在同一网段。如果不清楚网段相关知识，请咨询专业人士或者艾泰科技客户服务部。

3. 请确保所填写网关 MAC 地址正确，如果 MAC 地址填写错误，您将无法上网。

4.1.2.4 动态 IP 接入配置

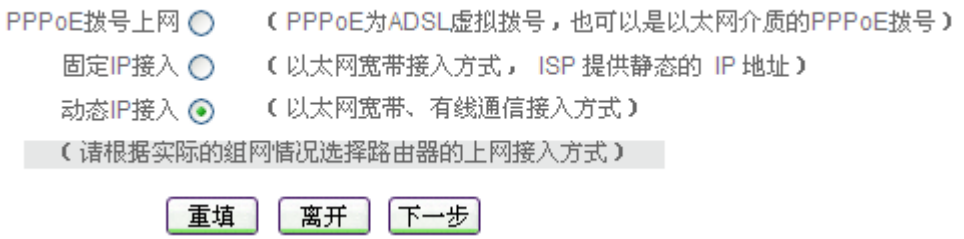


图 4-6 动态 IP 接入方式

在选择上网接入方式页面中，选中“动态 IP 接入”选项（如图 4-6），单击“下一步”按钮，进入动态 IP 接入页面（如图 4-7），在这里配置动态 IP 接入信息，单击“完成”按钮，动态 IP 接入线路配置完成，同时，系统密码、系统日期和系统时间也成功修改。

图 4-7 动态 IP 接入配置

- 局域网 IP 地址、子网掩码：配置成功后，该地址将作为局域网中计算机用作上网的网关地址（出厂值为 192.168.16.1/255.255.255.0）；
- 广域网接口 MAC 地址：一般情况下不需要设置。但是某些动态 IP 接入的时候（比

如有线通），Cable Modem 会记录下原先使用该线路的网络设备（如网卡）的 MAC 地址，这样会造成新的网络设备无法正常获得 IP 地址的现象，此时需要将新的网络设备（这里指设备）的 MAC 地址设置成和原有网络设备的 MAC 地址相同；

- 主 DNS 服务器：ISP（例如中国电信）提供的主用 DNS 服务器 IP 地址（可能会在线路刷新时更新成 ISP 分配的地址）；
- 备 DNS 服务器：ISP（例如中国电信）提供的备用 DNS 服务器 IP 地址。
- 启用 DNS 代理：选中之后，设备会启用 DNS 代理功能，此时给局域网中的计算机分配的主 DNS 服务器的 IP 地址就是设备局域网接口的 IP 地址。
- 上一步：返回到快速向导的第一页；
- 重填：恢复到修改前的动态 IP 配置参数；
- 离开：离开快速向导页面，进入主页面，快速向导所有操作无效；
- 完成：快速向导运行成功，所做的操作在这里生效。

提示：所做的操作，只有单击“完成”按钮才生效（包括快速向导的前一页）。

4.1.3 小结

配置好快速向导后，设备的一些最基本的功能已经配置完成。如果发现完成配置后不能上网，请检查各项配置是否正确，可以直接到***基本配置—>线路配置***（章节 5.1）中检查“默认线路”状态，查看、修改配置参数。

第5章 基本配置

设备除提供基本的上网共享功能外，还提供了一些附加的 IP 功能，方便配置、管理网络。本章主要讲述如何设置上网所需的基本网络参数，如线路配置、DHCP 和 DNS 服务器、接口配置以及 DDNS 服务。

5.1 线路配置

本节主要讲述***基本配置—>线路配置***的配置方法。

在本页面不仅可以配置多条线路，也可以根据实际需要修改或删除已配置的线路，还可以查看各条线路的连接状态信息。

在***快速向导***中配置完上网线路之后（注：在***快速向导***中只能配置“默认线路”），可以到本页面查看该线路的连接状态和配置情况，也可根据需要修改配置。如果是对我们的路由器配置比较熟练的用户，可以不经过***快速向导***而直接在本页面配置“默认线路”。

提示：若要使用多线路上网，在本页面配置各条线路之后，可到***基本配置—>线路组合***中配置线路组合的相关参数。

5.1.1 线路连接信息列表

在“线路连接信息列表”中可以查看各线路的配置及状态信息，如表 5-1、表 5-2 所示。

线路连接信息列表 1/10

1/1 第一页 上一页 下一页 最后页 前往 第 页 搜索

线路名称	物理接口	连接类型	连接状态	IP地址	子网掩码	网关地址
默认线路	WAN1	固定IP	已连接	200.200.202.132	255.255.255.0	200.200.202

刷新

表 5-1 线路连接信息列表

表 5-2 线路连接信息列表（续表 5-1）

5.1.1.1 参数涵义

- 线路名称：当前上网接入线路的名称；
- 物理接口：当前上网接入线路与设备相连的物理接口。注意，“默认线路”固定连接到 WAN1 口；
- 连接类型：当前上网接入线路的连接类型；特别地，如果是 PPPoE 拨号上网线路，同时还会显示该线路设置的“用户名”,；
- 连接状态：线路的当前连接状态。分以下三种情况：

1. PPPoE 拨号线路

如果当前线路是 PPPoE 拨号线路，那么，共有 8 种状态，详见表 5-3。处于“已连接”状态时，同时还会显示该线路保持本次连接的时间（单位：天:时:分:秒）。

连接状态	状态描述
关闭	物理接口没有连接，或者没有拨号
拨号中	拨号已经发起，但是服务方还未响应
验证中	服务方已经响应，正在验证用户名、密码
已连接	验证通过，PPPoE 连接已经建立，可以传送数据
断线中	正在拆除 PPPoE 连接
已挂机	一方已经发出挂机请求
已断线	PPPoE 连接已中断，等待拨号
内部错误	其它未定义状态

表 5-3 PPPoE 拨号线路连接状态描述

2. 固定 IP 接入线路

如果当前线路是固定 IP 接入线路，那么，共有 3 种状态，详见表 5-4。

连接状态	状态描述
关闭	物理接口没有连接
已连接	物理接口和对方网络设备建立连接
内部错误	其它未定义状态

表 5-4 固定 IP 接入线路连接状态描述

3. 动态 IP 接入线路

如果当前线路是动态 IP 接入线路，那么共有 3 种状态，详见表 5-5。处于“已连接”状态时，同时还会看到 ISP 给设备当前分配的 IP 地址的剩余租用时间（单位：天:时:分:秒）。

连接状态	状态描述
关闭	物理接口没有连接，或者已释放地址但尚未请求新地址
连接中	正在请求动态的 IP 地址
已连接	已经获得动态分配的 IP 地址，线路连接正常
内部错误	其它未定义状态

表 5-5 动态 IP 接入线路连接状态描述

- IP 地址、子网掩码、网关地址：分以下三种情况。

1. PPPoE 拨号线路

如果当前线路是 PPPoE 拨号线路，则它们分别为 ISP 当前分配的广域网接口的 IP 地址、子网掩码以及静态路由的网关地址；其中，“网关地址” 与“IP 地址”的值相同。

2. 固定 IP 接入

如果当前线路是固定 IP 接入线路，则分别为 ISP 提供的广域网接口的静态 IP 地址、子网掩码以及静态路由的网关地址。

3. 动态 IP 接入

如果当前线路是动态 IP 接入线路，则它们分别为 ISP 当前分配的广域网接口的 IP 地址、子网掩码以及静态路由的网关地址。

- 下行速率(bps)：在两次刷新列表的时间间隔内，当前线路实际的下行平均速率。单位：比特/秒；
- 上行速率(bps)：在两次刷新列表的时间间隔内，当前线路实际的上行平均速率。单位：比特/秒；

5.1.1.2 列表功能

- 增加线路：选中“添加”选项，如图 5-2 所示，输入线路相关配置信息，单击“保存”按钮，生成新的上网线路；

- 浏览线路：如果已经生成了若干上网线路，则可在“线路连接信息列表”中查看相关信息，如表 5-1、表 5-2 所示；
- 编辑线路：如果想编辑某条上网线路，只需单击该线路对应条目的“线路名称”超链接，其信息就会填充到相应的编辑框内，可修改它，再单击“保存”，修改完毕；
- 删除线路：如果想删除某条上网线路，首先需要单击该线路对应条目的“线路名称”超链接，然后才能执行删除线路操作，具体操作步骤请参考章节 5.1.2.4；
- 刷新：单击“刷新”按钮，可获得最新的线路连接信息。

5.1.1.3 PPPoE 拨号接入线路的拨号与挂断

如果某线路为 PPPoE 拨号接入线路，那么，在“线路连接信息列表”中单击该线路的“线路名称”超链接后，列表下方才会显示“拨号”和“挂断”按钮，如表 5-6、表 5-7 所示。这两个按钮的功能如下：

- 拨号：手动呼叫 PPPoE 连接，拨号过程中，在“连接状态”中可见“已断开”→“拨号中”→“验证中”→“已连接”四个过程。当 PPPoE 连接拨号类型设置为“手动拨号”时，需在这里完成 PPPoE 拨号；
- 挂断：手动挂断 PPPoE 连接，当 PPPoE 连接拨号类型设置为“手动拨号”时，需在这里挂断 PPPoE 连接。

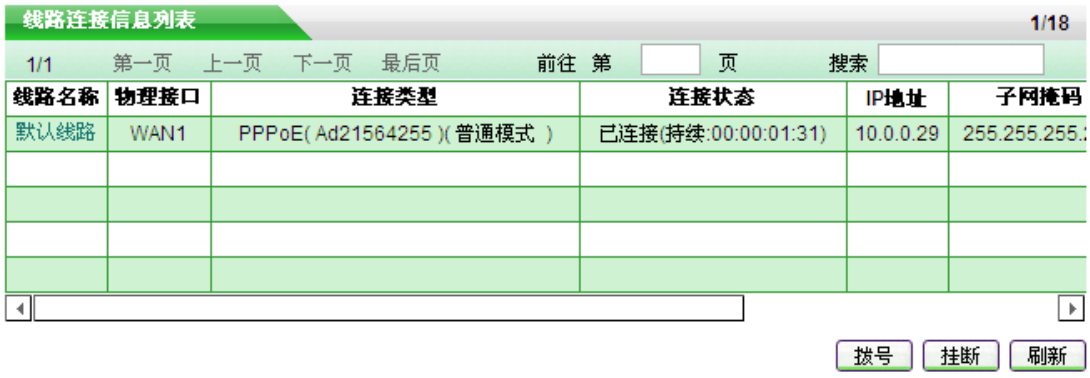


表 5-6 线路连接信息列表——PPPoE 拨号接入

表 5-7 线路连接信息列表——PPPoE 拨号接入（续表 5-6）

5.1.1.4 动态 IP 接入线路的更新与释放

如果某线路为动态 IP 接入线路，那么，在“线路连接信息列表”中单击该线路的“线路名称”超链接后，列表下方才会显示“更新”和“释放”按钮，如表 5-8、表 5-9 所示。这两个按钮的功能如下：

- 更新：系统自动完成一次先释放 IP 地址、再重新获得 IP 地址的过程（更新过程，在“连接状态”中可见“已断开”→“连接中”→“已连接”三个过程）；
- 释放：释放当前得到的动态 IP 地址。

线路连接信息列表
1/18
1/1 第一页 上一页 下一页 最后页 前往 第 页 搜索
线路名称 物理接口 连接类型 连接状态 IP地址 子网掩码 网
默认线路 WAN1 动态IP 已连接(剩余:00:00:59:59) 192.168.16.118 255.255.255.0 192
更新 释放 刷新

表 5-8 线路连接信息列表——动态 IP 接入

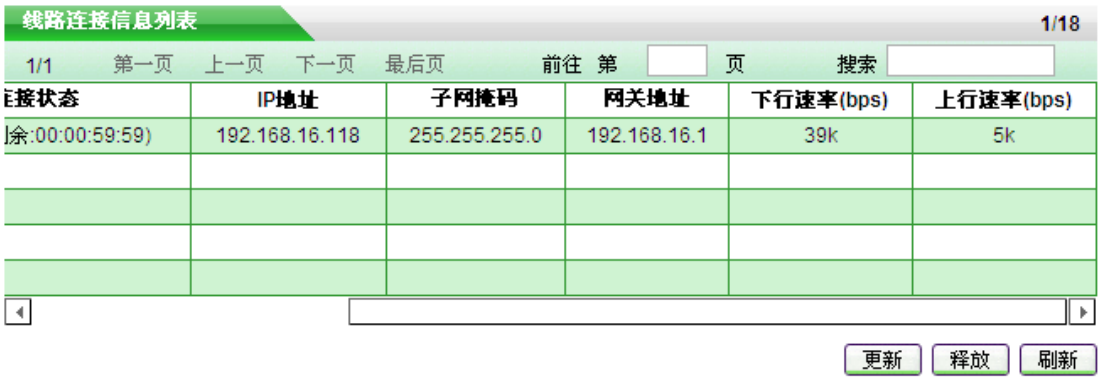

线路连接信息列表
1/18
1/1 第一页 上一页 下一页 最后页 前往 第 页 搜索
接状态 IP地址 子网掩码 网关地址 下行速率(bps) 上行速率(bps)
余:00:00:59:59) 192.168.16.118 255.255.255.0 192.168.16.1 39k 5k
更新 释放 刷新

表 5-9 线路连接信息列表——动态 IP 接入（续表 5-8）

5.1.2 线路配置

下面将首先分别介绍 PPPoE 拨号上网、固定 IP 接入、动态 IP 接入三种情况下，如何配置线路，以及如何删除已配置的线路。

提示：只有在配置完“默认线路”之后，才能配置其他上网线路。如果是直接在本页面配置“默认线路”，则首先需在“线路连接信息列表”中，单击“默认线路”超链接，然后才可以配置它。并且，“默认线路”固定连接到设备的 WAN1 口，其“线路名称”和“物理接口”禁止修改。其他线路的主 DNS 服务器为在默认线路中配置的主 DNS 服务器，不能修改。

5.1.2.1 PPPoE 拨号上网配置

图 5-1 PPPoE 拨号上网线路配置

- 线路名称：当前线路的名称（自定义，不能重复），取值范围：1~11 位字符；
- 物理接口：当前线路与设备相连的物理接口的名称；
- 连接类型：这里选中“PPPoE 拨号上网”；
- 用户名、密码：申请 PPPoE 业务的时候，ISP（例如中国电信）将提供上网账号及密码。如有疑问，请询问 ISP；

- 密码验证方式：ISP 验证用户名及密码的方式，多数地区为 PAP 方式，也有少数地区采用 CHAP 方式，NONE 表示不进行用户名和密码验证，Either 表示自动和对方设备协商采用哪种验证方式；
- 局域网 IP 地址、子网掩码：配置成功后，该地址将作为局域网中计算机用作上网的网关地址（出厂值为 192.168.16.1/255.255.255.0）；
- 服务名：ISP 提供的 PPPoE 服务名，一般不需要设置。如有疑问，请询问 ISP；
- 最大接收单元：缺省值为 1492 字节，PPPoE 拨号时设备将自动与对方设备协商，除非特别应用，不要修改；
- 拨号类型：

  自动拨号：当打开设备或者上一次拨号断线后自动拨号连接；

  手动拨号：由用户在***基本配置—>线路配置***的“线路连接信息列表”（章节 5.1.1）中手动进行连接和挂断；

  按需拨号：在局域网内部有访问 Internet 流量时设备自动进行连接；
- 拨号时段：允许 PPPoE 拨号的时间段（时间段在***带宽管理—>时间段***中配置），只有在此时间段内才允许 PPPoE 拨号。不设置代表不对拨号时段进行控制；
- 上线时段：允许设备上线连接到 Internet 的时间段（时间段在***带宽管理—>时间段***中配置），超出这个时间段的范围不允许设备上线；如果超出时间段时设备处于连接状态，它将自动断开 PPPoE 连接。不设置代表不对上线时段进行控制；
- 生命周期：在拨号成功后，系统将每隔 1000ms 向对端网络设备发送一个探测包，以探测线路是否可用，如果在“生命周期”范围内一直没有收到对方回应，则断开此连接，默认值：15000 毫秒；
- 空闲时间：无访问流量后自动断线前等待的时长，0 代表不自动断线（单位：秒）；
- 会话时间：连接生存时间，每次拨号成功到设置的时间后自动断线。一般情况下不要作此设置，0 代表没有时间限制（单位：秒）；
- 优先级：拨号成功后，该线路的路由优先级，目的网段相同的情况下，设备将优先选择优先级高的线路转发数据包，值越低优先级越高；
- 断开优先级：PPPoE 线路断开后，该线路的路由优先级，优先级高的优先拨号，值越低优先级越高；
- 拨号模式：选择 PPPoE 拨号的模式，默认为普通模式，在使用正确的用户名和密码的前提下，如果拨号不成功，可以尝试使用其它模式；
- 拨号子接口：子接口是指从属于某一个物理接口的逻辑上的虚接口，通常，在单个物理接口上可配置多个子接口。目前，设备仅支持在 WAN1 接口上配置多个子接口，不同子接口按照 802.1Q 值进行区分；
- DNS 服务器配置：系统提供两种 DNS 服务器配置方式：自动分配和手动配置。选择自动分配，设备将从 PPPoE 服务器端获取 DNS 服务器；选择手动配置，则需要用户手动输入主 DNS 服务器和备 DNS 服务器。

  1. 主 DNS 服务器：ISP（例如中国电信）提供的主用 DNS 服务器的 IP 地址，可不配置，线路连接成功后，设备将自动从 ISP 处获得；
  2. 备 DNS 服务器：ISP（例如中国电信）提供的备用 DNS 服务器的 IP 地址。

- 保存：PPPoE 拨号上网配置生效；

▶ 重填：恢复到修改前的配置参数。

提示：

1. 如果改变了“局域网 IP 地址”，在保存之后，必须使用新的 IP 地址重新登录设备才能进行 WEB 界面管理，并且局域网中所有计算机的默认网关必须设置成该 IP 地址才能正常上网；

2. 与在***基本配置—>快速向导***中提供的“PPPoE 拨号上网配置”（章节 4.1.2.2）相比较，这里提供了更多的配置参数，包括：“拨号时段”、“上线时段”、“生命周期”、“会话时间”、“优先级”、“断开优先级”等。而快速向导中也多提供了“启用 DNS 代理”的配置；

3. 在配置 PPPoE 拨号上网时，可以不配置主 DNS 服务器，PPPoE 拨号成功后，设备将自动从 ISP 处获得主 DNS 服务器的 IP 地址。

5.1.2.2 固定 IP 接入配置

图 5-2 固定 IP 接入线路配置

“线路名称”、“物理接口”这几个参数的涵义同“PPPoE 拨号上网配置”中的相关参数，这里不再重述。

- 连接类型：这里选中“固定 IP 接入”；
- 局域网 IP 地址、子网掩码：配置成功后，该地址将作为局域网中计算机用作上网的

网关地址（出厂值为 192.168.16.1/255.255.255.0）；

- 广域网 IP 地址、子网掩码、静态网关：申请固定 IP 接入业务的时候，ISP（例如中国电信）将提供设备对广域网的 IP 地址、子网掩码和静态网关；
- 网关绑定方式：绑定网关的 IP 地址和 MAC 地址，防止 WAN 口的 ARP 欺骗，默认为“不绑定”。选择“手工绑定”，输入网关 MAC 地址，将该 MAC 地址与网关的 IP 地址绑定。也可以通过获取按钮获取网关 MAC 地址。如不需要绑定网关，则选择“不绑定”。
- 主 DNS 服务器：ISP（例如中国电信）提供的主用 DNS 服务器的 IP 地址；
- 备 DNS 服务器：ISP（例如中国电信）提供的备用 DNS 服务器的 IP 地址。
- 获取：获取网关的 MAC 地址，当选择网关绑定方式为“手工绑定”时，单击“获取”按钮，可将网关的 MAC 地址填充到“网关 MAC 地址”文本框；
- 保存：固定 IP 接入配置生效；
- 重填：恢复到修改前的配置参数。
- **提示：**

1. 广域网 IP 地址、静态网关要在同一网段，某些 ISP（例如中国电信）给出的广域网 IP 地址和静态网关不在同一网段，请修改子网掩码的值，使它们处在同一网段。如果不清楚网段相关知识，请咨询专业人士或者艾泰科技客户服务部；

2. 如果改变了 “局域网 IP 地址”，在保存之后，必须使用新的 IP 地址重新登录设备才能进行 WEB 界面管理，并且，局域网中所有计算机的默认网关必须设置成该 IP 地址才能正常上网。

3. 请确保所填写的网关 MAC 地址正确，如果 MAC 地址填写错误，您将无法上网。

5.1.2.3 动态 IP 接入配置

图 5-3 动态 IP 接入线路配置

“线路名称”、“物理接口”这几个参数的涵义同“PPPoE 拨号上网配置”中的相关参数，这里不再重述。

- 连接类型：这里选中“动态 IP 接入”；
- 局域网 IP 地址、子网掩码：配置成功后，该地址将作为局域网中计算机用作上网的网关地址（出厂值为 192.168.16.1/255.255.255.0）；
- 广域网接口 MAC 地址：一般情况下不需要设置。但是某些动态 IP 接入的时候（比如有线通），Cable Modem 会记录下原先使用该线路的网络设备（如网卡）的 MAC 地址，这样会造成新的网络设备无法正常获 IP 地址的现象，此时需要将新的网络设备（这里指设备）的 MAC 地址设置成和原有网络设备的 MAC 地址相同；
- 主 DNS 服务器：ISP（例如中国电信）提供的主用 DNS 服务器的 IP 地址，在线路刷新时可能会更新成 ISP 分配的新地址；
- 备 DNS 服务器：ISP（例如中国电信）提供的备用 DNS 服务器的 IP 地址。
- 保存：动态 IP 接入配置生效；
- 重填：恢复到修改前的配置参数。

提示：如果改变了“局域网 IP 地址”，在保存之后，必须使用新的 IP 地址重新登录设备才能进行 WEB 界面管理，并且，局域网中所有计算机的默认网关必须设置成该 IP 地址才能正常上网。

5.1.2.4 删除线路

如果要删除某条线路，则需执行以下操作：

1. 在“线路连接信息列表”中，单击该线路对应条目的“线路名称”超链接，该线路相关信息即填充到编辑框中；

2. 在配置界面中，将“连接类型”选择为“删除线路”（如图 5-4），然后单击“保存”按钮；

图 5-4 删除线路

3. 单击“保存”按钮后，系统将弹出如图 5-5 所示对话框，再单击“确定”按钮，该

线路立即被删除。

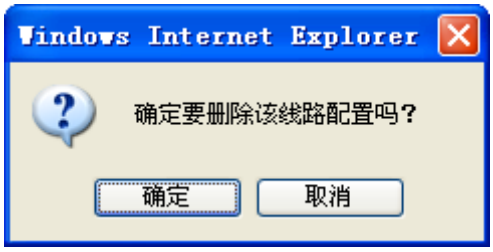


图 5-5 对话框——删除线路

提示：一次只能删除一条线路；并且，只有在没有任何其他线路时，才允许删除“默认线路”。

5.1.3 相关的缺省路由

在***快速向导***中配置完默认线路，或者在本页面中配置完默认线路和其他上网线路后，设备会自动生成各线路对应的缺省路由，可在***系统状态—>路由和端口信息***的“路由表信息列表”中查看到对应路由的状态信息，即目的地址为“0.0.0.0/0”的静态路由。

5.2 线路组合

本节主要讲述***基本配置—>线路组合***的配置方法。

在线路组合配置中，可以快速配置多线路上网的线路组合方式及其他相关参数，可以指定多条线路的线路检测方式，还可以为指定范围内的主机限制上网线路，并能通过不同的分配规则来控制线路流量。

注意：HiPER 510 不提供线路组合功能。

5.2.1 线路组合功能介绍

5.2.1.1 线路组合方式

设备提供了 2 个线路组：“主线路”组和“备份线路”组。为方便起见，将“主线路”组中的线路统称为主线路，将“备份线路”组中的线路统称为备份线路。所有线路缺省都是主线路，用户可以根据需要将某些线路划分到“备份线路”组中。但是，“默认线路”只能作为主线路使用。

设备提供了“所有线路负载均衡”和“部分线路负载均衡，其余备份”这两种线路组合方式。

在“所有线路负载均衡”方式下，所有线路都作为主线路使用。工作原理如下：

1. 当所有线路都正常时，局域网内主机将同时使用所有线路上网。

2. 若某条线路出现故障，则立即屏蔽该线路，原先通过该线路的流量将分配到其他线路上。

3. 一旦故障线路恢复正常，设备会自动启用该线路，流量自动重新分配。

在“部分线路负载均衡，其余备份”方式下，一部分线路作为主线路使用，另一部分线路则作为备份线路使用。工作原理如下：

1. 只要有一条（或更多）主线路正常，局域网内主机就使用主线路上网；此时，如果有多条主线路正常，那么，它们将按照负载均衡方式工作。

2. 若所有主线路都出现故障，则自动切换到使用备份线路上网；此时，如果有多条备份线路都正常，那么，它们也将按照负载均衡方式工作。

3. 一旦有一条（或更多）故障主线路恢复正常，则立即切换回主线路。

提示：当某条线路中断进行线路切换时，某些用户应用（比如部分网络游戏）可能会意外中断，这是由于 TCP 会话的属性决定的。艾泰科技将不承担由此引发的一切用户损失或者法律诉讼。

5.2.1.2 线路检测机制

无论采用哪种线路组合方式，要保证线路故障时网络不中断，都要求设备必须能够实时

地监控线路状态。为此，我们为设备设计了灵活的自动检测机制，并提供多种线路检测方法供用户选择，以满足实际应用的需要。

为方便理解，先介绍一下几个相关参数。

检测目标：检测的对象，设备将向预先指定的检测目标发送检测包以检测线路是否正常。

检测间隔：发送检测包的时间间隔，一次发送一个检测包，缺省值为 1000 毫秒。特别地，该值为 0 时，表示不进行线路检测。

检测次数：每个检测周期内，发送检测包的次数。

检测周期：该值为检测间隔与检测次数的乘积，例如，缺省情况下，该值为 1000×3＝3000 毫秒。

下面将分别介绍在线路正常和线路故障这两种情况下，设备的线路检测机制。

某条线路正常时，检测机制如下所述：设备将每隔指定的检测间隔向该线路的检测目标发送一个检测包，如果在某个检测周期内，发送的所有检测包都没有回应，就认为该线路出现故障，并立即屏蔽该线路。例如，缺省情况下，若某个检测周期内，发送的 3 个检测包都没有回应，就认为该线路出现故障。

某条线路故障时，检测机制如下所述：同样地，设备也是每隔指定的检测间隔向该线路的检测目标发送一个检测包，如果在某个检测周期内，发送的检测包中有一半及以上数量的检测包有回应时，就认为该线路已经正常，并恢复启用该线路。例如，缺省情况下，若某个检测周期内，有 2 个检测包有回应，就认为该线路恢复正常。

提示：允许不启用线路检测，这时需要将“检测间隔”设为“0”毫秒。

5.2.2 多线路负载均衡功能介绍

如章节 5.2.1.1 中所述，在设备中，无论使用哪种线路组合方式，当局域网主机正在使用的上网线路多于一条时，这些线路就会按照负载均衡方式工作。在以下各节中，我们将详细介绍设备的多线路负载均衡功能的特点。

5.2.2.1 根据源 IP 地址指定优先线路

设备允许用户预先为局域网中的某些主机指定上网线路，它是通过设置线路的“内部起始 IP 地址”和“内部结束 IP 地址”来实现的，IP 地址属于两个地址范围内的主机将优先使用指定线路。对于已指定上网线路的主机来说，当指定线路正常时，它们只能通过该线路上网；但是，当指定线路有故障时，它们会使用其他的正常线路上网。

5.2.2.2 根据线路带宽合理分配流量

设备中，用户能够预先指定分配到各条线路的流量的比例，它是通过设置线路的“权重”来实现的，“权重”大的线路将比“权重”小的线路承担更多流量。在实际应用中，一般可按线路的带宽比来设置各线路的“权重”，从而实现按线路带宽比合理分配流量。

例如，假设某用户申请了 4 根线路 A、B、C、D，带宽分别为 10M、6M、4M、4M。分为以下两种情况：

情况一，采用“所有线路负载均衡”方式，这 4 条线路均作为主线路使用，此时可将 A、B、C、D 的“权重”分别设置为 5、3、2、2；

情况二，采用“部分线路负载均衡，其余备份”方式，不妨假设 A 和 B 作为主线路使用、C 和 D 作为备份线路使用，则可将 A、B 的“权重”分别设置为 5、3，将 C 和 D 的“权重”都设置为 1。

需要注意的是，当局域网中的某些主机指定了上网线路时，若按照带宽比来设置线路的“权重”，线路的实际流量比可能会同带宽比相差较大。这时，可以根据实际情况适当调整各线路的“权重”。

5.2.2.3 提供两种流量分配规则

“分配规则”用来控制线路流量，它作用于局域网中没有指定上网线路的计算机，设备提供两种分配规则：“NAT 会话”和“IP 地址”，它们的实现机制如下所述：

1. IP 地址

使用 IP 地址作为分配规则时，设备将根据线路的“权重”，把未指定上网线路的主机的 IP 地址，按顺序依次分配到当前正在使用的各条线路上。分配到各条线路的 IP 地址的数量比（即主机数量比）为线路的“权重”比，来自同一个 IP 地址的 NAT 会话使用同一条线路。

例如，若当前同时使用 3 条线路上网，“权重” 分别为 3、2、1，则根据连接的先后顺序，第 1、2、3 台上网的主机将使用第一条线路，第 4、5 台主机将使用第二条线路，第 6 台主机将使用第三条线路，接着第 7、8、9 台主机将使用第一条线路，……，依此类推。注意，这里假设每台主机均只有一个 IP 地址。

2. NAT 会话

使用 NAT 会话作为分配规则时，设备将根据线路的“权重”，把未指定上网线路的主机发起的 NAT 会话，按顺序依次分配到当前正在使用的各条线路上。分配到各线路的 NAT 会话的数量比为线路的“权重”比，同一主机发起的 NAT 会话可使用多条线路。

例如，若当前同时使用 3 条线路上网，“权重” 分别为 3、2、1，则根据连接的先后顺序，内网主机发起的第 1、2、3 个 NAT 会话将使用第一条线路，第 4、5 个 NAT 会话将使用第二条线路，第 6 个 NAT 会话将使用第三条线路，接着第 7、8、9 个 NAT 会话将使用第一条线路，……，依此类推。

一般情况下，建议“分配规则”选择为“IP 地址”。当对带宽要求高，需要多线路带宽合并时，比如使用网络蚂蚁（NetAnts）、网际快车（FlashGet）、影像传送带（Net Transport）等多线程下载工具时（多线程下载指把一个下载文件分成若干份同时下载，下载后再把它们合并起来），则可选择“NAT 会话”，从而能够充分利用多线路带宽，以提高下载速度。需要注意的是，即便选择了“NAT 会话”，由于网站情况不同仍有可能造成带宽不能完全叠加的情况，同时还可能造成某些应用连接不畅。

5.2.3 线路组合通用设置

由于“所有线路负载均衡”和“部分线路负载均衡，其余备份”这两种线路组合方式下，通用设置的界面不同，因此，以下将分别介绍它们的通用设置参数。

5.2.3.1 所有线路负载均衡

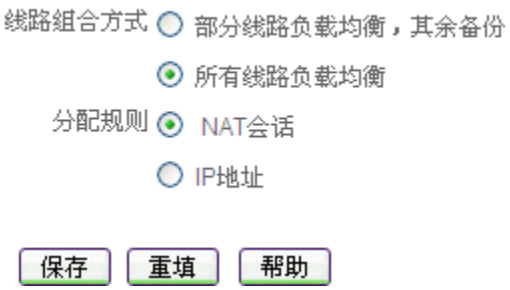


图 5-6 线路组合通用配置——所有线路负载均衡

- 线路组合方式：这里选中“所有线路负载均衡”。具体描述请参见章节 5.2.1.1；
- 分配规则：控制线路流量时使用的规则。选项为“NAT 会话”或“IP 地址”，缺省值为“IP 地址”。具体描述请参见章节 5.2.2.3。
- 保存：线路组合配置参数生效；
- 重填：恢复到修改前的配置参数。

5.2.3.2 部分线路负载均衡，其余备份

图 5-7 线路组合配置——部分线路负载均衡，其余备份

“线路检测方法”、“分配规则”这两个参数的涵义，与“所有线路负载均衡”方式下相关参数涵义相同，这里不再重述。

- 线路组合方式：这里选中“部分线路负载均衡，其余备份”。具体描述请参见章节 5.2.1.1；
- 主线路：该列表框代表“主线路”组，位于该列表框中的线路全部都作为主线路使用；
- 备份线路：该列表框中代表“备份线路”组，位于该列表框中的线路全部都作为备份线路使用。

- ==>（向右箭头）、<==（向左箭头）：首先在“主线路”列表框中选中一条（或更多）线路，然后单击“==>”按钮，被选中的线路立即被移到“备份线路”列表框中。类似地，首先在“备份线路”列表框中选中一条（或更多）线路，然后单击“<==”按钮，被选中的立即被移到“主线路”列表框中。
- 保存：线路组合配置参数生效；
- 重填：恢复到修改前的配置参数。

提示：

1. 默认线路只能位于“主线路”列表框中，不能移到“备份线路”列表框中；

2. 本方式下，若将“线路组合方式”修改成“所有线路负载均衡”，单击“保存”按钮后，系统立即将“备份线路”列表框中的所有线路都移到“主线路”列表框中；

3. 本方式下，若“备份线路”列表框中所有线路都被移到“主线路”列表框中，单击“保存”按钮后，或者若用户删除了所有的备份线路，“线路组合方式”将自动切换为“所有线路负载均衡”。

5.2.4 线路检测及权重配置

提示：在这里可以分别设置各条线路的线路组合信息（即线路检测、负载均衡）相关参数的配置。在配置前，首先需要在“线路组合信息列表”（如表 5-11）中，单击欲配置线路的“线路名称”超链接，其相关信息填充到相应的编辑框以后，然后才可以配置该线路。

图 5-8 线路检测及权重配置

- 检测目标类型：欲检测的目标的类型，选项为“网关”、“其他”。ARP 方式下，仅支持检测“网关”；DNS 方式下，仅支持检测“其他”；ICMP 方式下，两个都支持。
  网关：线路的检测目标为该线路下一跳网关；
  其他：线路的检测目标为用户自定义的其他检测目标；
- 检测间隔：发送检测包的时间间隔，单位：毫秒。启用线路检测时，取值范围为 1000～60000，缺省值为 1000。该值为 0 时，表示不启用线路检测；
- 检测次数：检测周期内发送检测包的次数（每次发送一个检测包）。缺省值为 10；
- 检测目标 IP 地址：欲检测的目标的 IP 地址。当“检测目标类型”为“其他”时，

需配置该参数；“检测目标类型”为“网关”时，无需配置，此时，网关地址就是检测目标 IP 地址；

- 权重：当前线路的权重，取值范围为 1~255，缺省值为 1。具体描述请参见章节 5.2.2.2；
- 内部起始 IP 地址、内部结束 IP 地址：局域网内优先使用当前线路上网的主机的起始 IP 地址和结束 IP 地址。具体描述请参见章节 5.2.2.1。
- 保存：上述配置参数生效；
- 重填：恢复到修改前的配置参数。

提示：

1. “检测目标类型”、“检测间隔”、“检测次数”以及“检测目标 IP 地址”为线路检测相关参数，更详细的说明请参见章节 5.2.1.2；

2. “权重”、“内部起始 IP 地址”以及“内部结束 IP 地址”为负载均衡相关参数，更详细的说明请参见章节 5.2.2.1、章节 5.2.2.2。

5.2.5 线路组合信息列表

线路名称	连接类型	主/备	权重	连接状态	NAT会话比	IP地址	检
默认线路	固定IP	主线路	1	已连接(√)	100%	200.200.202.131	
test	PPPoE	主线路	1	关闭	0%		

表 5-10 线路组合信息列表

:	检测目标类型	检测目标IP地址	检测间隔	检测次数	内部起始IP地址
2.131	网关	0.0.0.0	0	10	0.0.0.0
	网关	0.0.0.0	0	3	0.0.0.0

表 5-11 线路组合信息列表（续表 5-11）

5.2.5.1 部分参数涵义

“线路名称”、“连接类型”、“连接状态”、“IP 地址”这几个参数的涵义同***基本配置—>***

线路配置的“线路连接信息列表”（章节 5.1.1）的相关参数，其中，若“连接状态”显示为“已连接（*）”，则表示该线路连接正常，但是并未使用；若“连接状态”显示为“已连接（√）”，则表示该线路连接正常，并且正在使用。

“NAT 会话比”、“上行流量比”、“下行流量比”的涵义如下：

- NAT 会话比：在两次刷新本列表的时间间隔（即统计时长）内，通过此线路建立的 NAT 会话的数量占所有线路建立的 NAT 会话的总数量的百分比。
  使用单线路上网时，在统计时长内，如果没有建立新的 NAT 会话，则该值为“0%”；否则，该值为“100%”。
  使用多线路上网时，在统计时长内，如果通过此线路没有建立新的 NAT 会话，则该值为“0%”；否则，按实际百分比显示。

5.2.5.2 列表功能

- 编辑线路组合信息：如果想编辑某条线路的线路组合信息的相关参数，只需单击该线路对应条目的“线路名称”超链接，其信息就会填充到相应的编辑框内（如图 5-2），可修改它，再单击“保存”按钮，修改完毕；
- 浏览线路组合信息：如果已经配置了若干线路的线路组合信息，则可以在“线路组合信息列表”中查看相关信息，如表 5-11、5-12 所示；
- 刷新：单击“刷新”按钮，可获得最新的线路组合信息。

5.2.6 配置线路组合

5.2.6.1 线路组合的配置顺序

只有在使用多线路上网的情况下，才需配置线路组合相关参数。配置顺序如下：

1. 进入***基本配置—>线路配置***（章节 5.1.2）页面，首先配置“默认线路”，然后根据需要配置其他自定义线路（也可在***开始***菜单配置线路）。注意，“默认线路”也可以直接在***基本配置—>快速向导***（章节 4.1）中配置；

2. 进入***基本配置—>线路组合***页面，根据需要进行线路组合通用设置，具体步骤请参见章节 5.2.6.2；

3. 在***基本配置—>线路组合***页面中，根据需要分别配置各条线路的线路组合信息的相关参数，具体步骤请参见章节 5.2.6.3。

5.2.6.2 线路组合通用设置配置步骤

第一步，进入***基本配置—>线路组合***页面；

第二步，根据需要，设置“线路组合方式”；如果“线路组合方式”选择为“部分线路负载均衡，其余备份”时，还应根据实际需求将“主线路”列表框中的若干线路移到“备份线路”列表框中；

第三步，根据需要，设置“分配规则”；

第四步，单击“保存”按钮，通用设置相关参数配置完成。

5.2.6.3 线路检测及权重配置步骤

第一步，进入***基本配置—>线路组合***页面；

第二步，根据需要，在“线路组合信息列表”中，单击欲配置线路的“线路名称”超链接；

第三步，根据需要，设置该线路的线路检测相关参数，包括：“检测目标类型”、“检测间隔”、“检测次数”以及“检测目标 IP 地址”等；

第四步，根据需要，设置该线路的负载均衡相关参数，包括：“权重”、“内部起始 IP 地址”以及“内部结束 IP 地址”等；

第五步，单击“保存”按钮，该线路的线路组合信息相关参数配置完成；

第六步，如果还需配置其他线路，则重复第二步至第五步。

5.2.7 相关的检测路由

当默认线路或其他某条上网线路启用线路检测后，系统还会自动生成相应的检测路由，从而保证检测包是通过当前待检测的线路转发的。可在***高级配置—>路由配置***（章节 6.2）的“路由信息列表”中查看对应路由的配置信息，具体描述详见章节 6.2.2。

提示：对于固定 IP 或动态 IP 接入线路来说，当“检测目标”为“网关”时，系统将直接使用该线路对应的缺省路由来转发检测包，即该缺省路由同时也作为检测路由来使用。

5.3 DHCP 和 DNS 服务器

本节主要讲述***基本配置—>DHCP 和 DNS 服务器***的配置方法。

TCP/IP 协议设置包括 IP 地址、子网掩码、网关、DNS 服务器以及一些扩展信息等。为局域网中的所有计算机正确配置 TCP/IP 协议是一件非常繁琐的事情。设备能够配置成 DHCP 服务器，为局域网计算机动态分配 IP 地址、子网掩码、网关、以及 DNS 服务器、WINS 服务器等信息。

5.3.1 DHCP 服务配置

图 5-9 DHCP 服务配置

- 启用 DHCP 服务器：用来禁用或允许设备的 DHCP 服务器功能。选中为允许，如图 5-9 所示；
- 起始 IP 地址：DHCP 服务器给局域网计算机自动分配的起始 IP 地址（一般要和设备的局域网接口的 IP 地址在一个网段）；
- 子网掩码：DHCP 服务器给局域网计算机自动分配的子网掩码（一般要和设备局域网接口的子网掩码一致）；
- 总地址数：DHCP 服务器可以分配的地址总数量；
- 网关地址：DHCP 服务器给局域网计算机自动分配的网关 IP 地址（一般要和设备的局域网接口的 IP 地址一致）；
- 租用时间：局域网计算机获得设备分配的 IP 地址的租用时间（单位：秒）；
- 主 DNS 服务器：DHCP 服务器给局域网计算机自动分配的主用 DNS 服务器的 IP 地址，此处会自动识别在***基本配置—>快速向导***或者在***基本配置—>线路配置***默认线路设置的值；
- 备 DNS 服务器：DHCP 服务器给局域网计算机自动分配的备用 DNS 服务器的 IP 地

址，此处会自动识别在***基本配置—>快速向导***或者在***基本配置—>线路配置***中默认线路设置的值；

- 启用 DNS 代理：选中之后，设备会启用 DNS 代理功能，此时给局域网中的计算机分配的主 DNS 服务器的 IP 地址就是设备局域网接口的 IP 地址。
- 保存：DHCP 服务器配置参数生效；
- 重填：恢复到修改前的配置参数。

提示：

1. 启用了 DNS 代理功能之后，必须要设置一个 ISP（例如中国电信）提供的可用的“主 DNS 服务器”；

2. 如果要使用设备的 DHCP 服务器功能，局域网计算机的 TCP/IP 协议必须设置为“自动获得 IP 地址”；

3. 如果用户原先使用的是代理服务器软件（如 wingate），且计算机的 DNS 服务器设置为代理服务器的 IP 地址，那么，只需将设备的局域网接口的 IP 地址设置为同一个 IP 地址，这样，当设备启用 DNS 代理功能之后，用户不需要修改计算机的配置就可以转换到使用设备的 DNS 代理功能了。

5.3.2 DHCP 地址池使用信息

表 5-12 DHCP 地址使用信息列表

显示 DHCP 地址池使用信息：选中后，系统将显示“DHCP 地址使用信息列表”，如表 5-12 所示；

- ID：地址使用者的序号；
- IP 地址：DHCP 服务器分配的 IP 地址；
- MAC 地址：使用该 IP 地址的网络设备的 MAC 地址。“?????pending?????”表示该 IP 地址在租期时间范围内，但该网络设备已经离线，如果在租期内该网络设备再次申请 IP 地址，仍将获得该 IP 地址；
- 掩码：DHCP 服务器分配的 IP 地址的子网掩码；
- 剩余租期：租用该 IP 地址的剩余时间（时间单位：天:时:分:秒）；
- 刷新：单击“刷新”按钮，可获得最新的 DHCP 地址池使用信息。

5.3.3 配置 DHCP 服务器

第一步，进入***基本配置—>DHCP 和 DNS 服务器***页面；

第二步，选中“启用 DHCP 服务器”选项，根据需要填写“起始 IP 地址”、“子网掩码”、“总地址数”、“网关地址”、“租用时间”、“主 DNS 服务器”、“备 DNS 服务器”等信息；

第三步，若希望启用设备的 DNS 代理功能，则需选中“启用 DNS 代理”，此时局域网中计算机分配到的 DNS 服务器是设备局域网接口的 IP 地址；

第四步，单击“保存”按钮，DHCP 服务器配置生效。

提示：如果要关闭 DHCP 服务器功能，请取消“启用 DHCP 服务器”的选中，单击“保存”按钮。

5.4 接口配置

本节主要讲述*基本配置—>接口配置*的配置方法。

5.4.1 接口配置

在本页面，可以修改设备的物理接口的 IP 地址、MAC 地址及工作模式，如图 5-10 所示。

图 5-10 接口配置

- 选择接口：欲配置的接口的名称；
- IP 地址：该接口的 IP 地址；
- 子网掩码：该接口的子网掩码；
- MAC 地址：该接口的 MAC 地址（一般情况下不需要修改）；
- 模式：该接口的工作模式。Auto—自适应，100MFD—100M 全双工，100MHD—100M 半双工，10MFD—10M 全双工，10MHD—10M 半双工。一般情况下不需要修改，如有兼容性问题，或使用的设备不支持自动协商功能，可以在这里设置以太网协商的类型。
- 保存：接口配置参数生效；
- 重填：恢复到修改前的配置参数。

提示：

1. 设备支持为每个物理接口配置两个不同网段的 IP 地址，支持连接两个不同的网段，而且可以相互通讯；

2. 如果改变了 LAN 口的“IP 地址”，在保存之后，必须使用新的 IP 地址才能登录 WEB 界面管理，并且，局域网中计算机的默认网关必须设置成该 IP 地址才能正常上网；

5.4.2 接口配置信息列表

表 5-13 接口配置信息列表

- 浏览接口配置信息：如果已经配置了各个接口的相关信息，可在“接口配置信息列表”中查看各个接口配置状态信息，如表 5-13 所示；
- 编辑接口配置信息：如果需要编辑修改某个接口的配置信息，则首先在配置界面的“选择接口”中选中该接口的名称，或者在“接口配置信息列表”中单击对应条目的“接口名称”超链接，其信息就会填充到相应的编辑框内，然后即可修改该接口的相关信息；
- 刷新：单击“刷新”按钮，可查看最新的接口配置信息。

5.4.3 配置 IP 地址

第一步，进入***基本配置—>接口配置***页面；

第二步，选择需要配置 IP 地址的物理接口；

第三步，设置该接口的 IP 地址和子网掩码：在“IP 地址”中填入 IP 地址，在“子网掩码”中填入子网掩码；

第四步，单击“保存”按钮，配置完成。

提示：在这里可以快速配置、修改各接口的 IP 地址和子网掩码。

5.4.4 配置 MAC 地址

第一步，进入***基本配置—>接口配置***页面；

第二步，选择需要配置 MAC 地址的物理接口；

第三步，设置该接口的 MAC 地址：在“MAC 地址”中填入该接口的 MAC 地址；

第四步，单击“保存”按钮，配置完成。

提示：一般情况下，不需要配置 MAC 地址。但是某些动态 IP 接入的时候（比如有线通），Cable Modem 会记录下原先使用该线路的网络设备（如网卡）的 MAC 地址，这样会造成新的网络设备无法正常获得 IP 地址的现象，此时需要将新的网络设备的 MAC 地址

设置成和原有网络设备的 MAC 地址相同。

5.4.5 配置以太网工作模式

第一步，进入***基本配置—>接口配置***页面；

第二步，选择需要配置以太网工作模式的物理接口；

第三步，设置该接口的工作模式：在“模式”中选择工作模式。

第四步，单击“保存”按钮，配置完成。

提示：一般情况下，不需要修改，即接口默认自适应工作模式。如有兼容性问题，或使用的设备不支持自动协商功能，才需要设置该接口的工作模式。

5.5 DDNS 配置

本节主要讲述***基本配置—>DDNS 配置***的配置方法。

提示：只有在***系统管理—>时钟管理***中正确配置了设备的系统时间和时区信息，DDNS 功能才能正常工作。

动态域名解析服务（DDNS）是将一个固定的域名解析成动态变化的 IP 地址（如 ADSL 拨号上网）的一种服务。需向 DDNS 服务提供商申请这项服务，DDNS 的具体服务由各服务商根据实际情况提供。各 DDNS 服务提供商保留随时变更、中断或终止部分或全部网络服务的权利。目前，DDNS 服务是免费的，DDNS 服务提供商在提供网络服务时，可能会对使用 DDNS 服务收取一定的费用。在此情况下，艾泰科技会尽可能及时通知。如拒绝支付该等费用，则不能使用相关的服务。在免费阶段，艾泰科技不担保 DDNS 服务一定能满足要求，也不担保网络服务不会中断，对网络服务的及时性、安全性、准确性也都不作担保。

目前，艾泰科技提供对 3322.org 的 DDNS 服务的支持，将来还将陆续提供对其他 DDNS 服务的支持。

5.5.1 申请 DDNS 帐号

请登录 http://www.3322.org 申请后缀名为 3322.org 的二级域名。

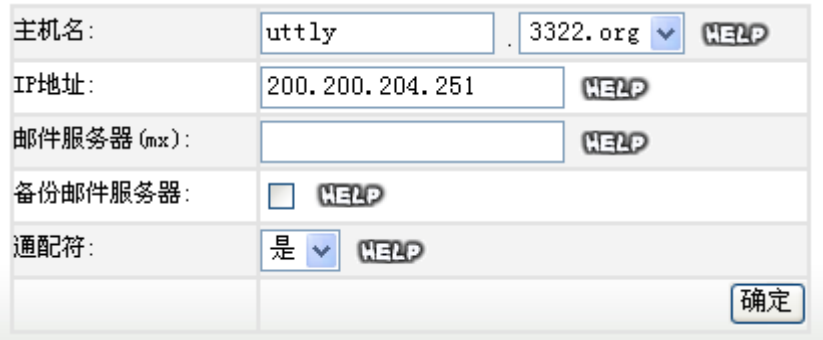


图 5-11 申请 DDNS 帐号

- 主机名：填入欲申请的二级域名，不能与已注册的域名重复；
- IP 地址：当前域名对应的 IP 地址；
- 确定：单击“确定”按钮，成功注册域名。

5.5.2 配置 DDNS 服务

图 5-12 配置 DDNS 服务

- 接口：选择配置 DDNS 服务的接口，设备的所有 WAN 口都可以配置 DDNS 服务；
- 启用 DDNS 服务：启用或者禁用 DDNS 服务，选中为启用；
- 注册域名：单击 http://www.3322.org 超链接，即可进入该页面申请域名；
- 服务商：选择提供域名服务的服务商此处选择 3322.org；
- 主机名：申请 DDNS 帐号时使用的主机名。
- 用户名：用户注册时输入的用户名；
- 口令：用户注册时系统生成的密码；
- 保存：DDNS 配置生效；
- 重填：恢复到修改前的配置参数；
- 更新状态：单击“更新状态”按钮，可将当前接口的 IP 地址更新到域名系统中，如下表所示。

状态更新信息列表 1/1

1/1 第一页 上一页 下一页 最后页 前往 第 页 搜索

接口名称	更新状态	主机名	IP地址	更新时间
WAN1	更新成功	uttly.3322.org	200.200.204.251	Mon, 2 Feb 2009 05:47:13 GMT

表 5-14 DDNS 状态

5.5.3 DDNS 验证

可以在局域网计算机上执行命令提示符程序，使用 Ping 命令（例如：ping uttly.3322.org）检查 DDNS 是否更新成功。看到正确解析出 IP 地址（例如：200.200.204.251），证明域名解析正确。注意：一般情况下，设备在使用 NAT 后，从 Internet 上将不能 ping 通设备的 IP 地址，只能解析出该域名对应的 IP 地址。

```
C:\>ping uttly.3322.org

Pinging uttly.3322.org [200.200.204.251] with 32 bytes of data:

Reply from 200.200.204.251: bytes=32 time<1ms TTL=255
Reply from 200.200.204.251: bytes=32 time<1ms TTL=255
Reply from 200.200.204.251: bytes=32 time<1ms TTL=255
Reply from 200.200.204.251: bytes=32 time<1ms TTL=255

Ping statistics for 200.200.204.251:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

1. ISP（例如中国电信）分配给 WAN 口连接线路的 IP 地址是公网地址的时候才能保证该域名能被 Internet 的用户访问；

2. DDNS 功能可以帮助动态 IP 使用 VPN 和服务器映射。

第6章 高级配置

本章主要讲述如何设置设备的端口映射和虚拟服务器、路由配置、IP/MAC 绑定、UPnP 以及即插即用能等高级属性的相关参数。

6.1 端口映射和虚拟服务器

本节主要讲述*高级配置—>端口映射和虚拟服务器*的配置方法。

6.1.1 NAT 功能介绍

6.1.1.1 NAT 简介

NAT（网络地址转换）是一种将一个 IP 地址域（如 Intranet）映射到另一个 IP 地址域（如 Internet）的技术。NAT 的出现是为了解决 IP 日益短缺的问题，NAT 允许专用网络在内部使用任意范围的 IP 地址，而对于公用的 Internet 则表现为有限的公网 IP 地址范围。由于内部网络能有效地与外界隔离开，所以 NAT 也可以对网络的安全性提供一些保证。

设备提供了灵活的 NAT 功能，以下各节将详细介绍它的特点。

6.1.1.2 NAT 地址空间

为了正确进行 NAT 操作，任何 NAT 设备都必须维护两个地址空间：一个是局域网主机在内部使用的私有 IP 地址，设备中用“内部 IP 地址”表示；另一个是用于外部的公网 IP 地址，设备中用“外部 IP 地址”表示。

6.1.1.3 端口映射和虚拟服务器（DMZ 主机）

启用 NAT 功能后，设备会阻断从外部发起的访问请求。然而，某些应用环境下，广域网中的计算机希望通过设备访问局域网内部服务器，这时，就需要在设备上设置端口映射或虚拟服务器（DMZ 主机）来达到这个目的。

1. 端口映射

通过端口映射功能，可建立**<外部 IP 地址+外部端口>**与**<内部 IP 地址+内部端口>**一对一的映射关系，这样，所有对设备某指定端口的服务请求都会被转发到匹配的局域网服务器上，从而，广域网中的计算机就可以访问这台服务器提供的服务了。

2. 虚拟服务器（DMZ 主机）

某些情况下，需要将一台局域网计算机完全暴露给 Internet，以实现双向通信，这时候就需要将该计算机设置成虚拟服务器（DMZ 主机）。当有外部用户访问该虚拟服务器所映射

的公网地址时，设备会直接把数据包转发到该虚拟服务器上。

提示：被设置为虚拟服务器的计算机将失去设备的保护功能。

3. 匹配优先级

端口映射的优先级高于虚拟服务器。当设备收到一个来自外部网络的请求时，它将首先根据外部访问请求的 IP 地址及端口号，检查是否有匹配的端口映射，如果有的话，就把请求消息发送到该端口映射匹配的局域网计算机上。如果没有匹配的静态映射，才会检查是否有匹配的虚拟服务器。

6.1.1.4 对称 NAT

对称 NAT，即 Symmetric NAT，每一个来自相同内部 IP 与 port 的请求到一个特定目的地的 IP 地址和端口，映射到一个独特的外部来源的 IP 地址和端口。 同一个内部主机发出一个信息包到不同的目的端，不同的映射使用端口映射。

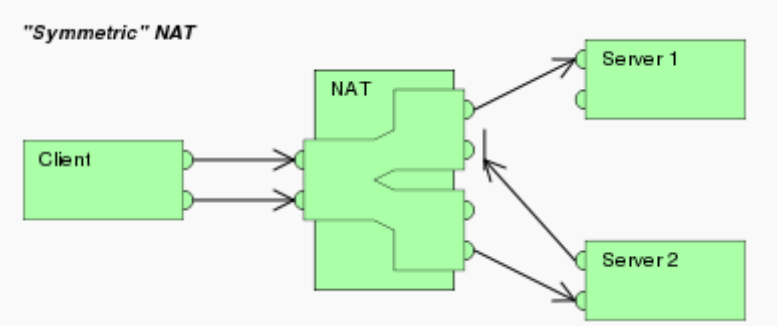


图 6-1 对称 NAT 简介

6.1.1.5 端口映射配置

图 6-2 端口映射配置

- 端口映射名：端口映射的名称（自定义，不能重复）。取值范围：1～11 个字符；
- 协议：数据包的协议类型，可供选择的有：TCP、UDP 和 GRE；
- 端口：设备提供给 Internet 的服务端口；
- IP 地址：局域网中作为服务器的计算机的 IP 地址；
- 保存：端口映射配置参数生效；
- 重填：恢复到修改前的配置参数。

提示：

1. 系统某些功能（*系统管理—>远程管理*）会添加一些默认 NAT 映射，在本页面无法编辑或删除它们；
2. 设备提供的端口映射功能内部端口和外部端口保持一致。即所填入的端口既为内部端口也为外部端口。

6.1.1.6 端口映射列表

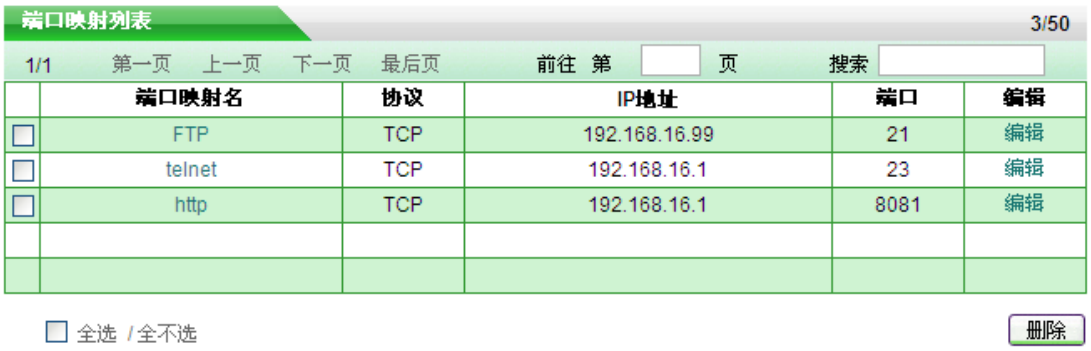


表 6-1 端口映射列表

- 增加端口映射：选中“添加”选项，输入端口映射信息，单击“保存”按钮，生成新的端口映射；
- 浏览端口映射：如果已经生成了端口映射，则可在“端口映射列表”中浏览端口映射信息；
- 编辑端口映射：如果想编辑某条端口映射，只需单击该端口映射的“端口映射名”或“编辑”超链接，其信息就会填充到相应的编辑框内，然后修改它，再单击“保存”按钮，修改完毕；
- 删除端口映射：选中一些端口映射，单击右下角的“删除”按钮，即可删除被选中的端口映射。

6.1.1.7 自定义端口映射

第一步，进入*高级配置—>端口映射和虚拟服务器*页面；

第二步，在“端口映射”配置栏，选择“添加”选项，填写“端口映射名”；

第三步，根据需要填写局域网服务器的“IP 地址”，所开服务的“协议”和“端口”；

第四步，单击“保存”按钮，该端口映射添加成功。可以在“端口映射列表”中看到相应的记录；

第五步，继续配置其他的端口映射。

提示：删除端口映射，在“端口映射列表”中选中要删除的端口映射，单击“删除”按钮，即可删除被选中的端口映射。

6.1.1.8 端口映射配置实例

局域网计算机 192.168.16.99 开设了 TCP21 端口的服务，但是希望外部通过 21 端口访

问这个服务，具体配置如下图所示：

图 6-3 端口映射配置——实例一

6.1.2 虚拟服务器配置

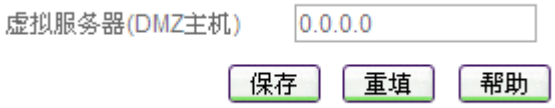


图 6-4 NAT 全局配置

- 虚拟服务器（DMZ 主机）：欲用作虚拟服务器（DMZ 主机）的局域网计算机的 IP 地址，此处配置的是全局虚拟服务器。
- 保存：虚拟服务器配置参数生效；
- 重填：恢复到修改前的配置参数。

6.1.3 对称 NAT

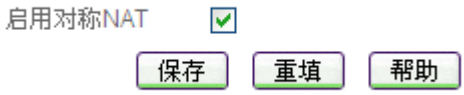


图 6-5 对称 NAT 配置

- 启用对称 NAT：选中表示启用对称 NAT，默认为关闭。当用户配置了双线路，设备将自动开启此功能；而删除了线路仅保留一条线路时，对称 NAT 则自动关闭。
- 保存：虚拟服务器配置参数生效；
- 重填：恢复到修改前的配置参数。

6.2 路由配置

本节主要讲述***高级配置—>路由配置***的配置方法。

6.2.1 静态路由概述

在本页面可配置静态路由，静态路由就是由网络管理员手工配置的路由，使得到指定目的网络的数据包的传送，按照预定的路径进行。静态路由不会随未来网络结构的改变而改变，因此，当网络结构发生变化或出现网络故障时，需要手工修改路由表中相关的静态路由信息。

正确设置和使用静态路由可以改进网络的性能，还可以实现特别的要求，比如实现流量控制、为重要的应用保证带宽等。

6.2.2 系统保留路由

在设备中，有两类保留的静态路由：缺省路由和检测路由，以下两节将分别介绍它们。用户自定义其他静态路由时，不允许使用保留路由名。

1. 缺省路由

缺省路由是一种特殊的静态路由，简单地说，就是在没有找到匹配的路由时使用的路由。在路由表中，缺省路由以目的网络为 0.0.0.0、子网掩码为 0.0.0.0 的形式出现。如果数据包的目的地址不能与任何路由相匹配，那么系统将使用缺省路由转发该数据包。

在***基本配置—>快速向导***中配置完默认线路，或者在***基本配置—>线路配置***中配置完默认线路和其他上网线路后，系统会自动生成各线路对应的缺省路由，可在***系统状态—>路由和端口信息***的“路由表信息列表”查看到对应路由的状态信息，即目标地址为“0.0.0.0/0”的静态路由。

如果上网线路为固定 IP 或动态 IP 接入线路，还可在本页面的“路由信息列表”中查看到对应路由的配置信息。不同情况下，各条上网线路对应的缺省路由的名称不同，具体信息参见表 7-4。

提示：“默认线路”固定接到设备的 WAN 口。

上网线路			缺省路由名
线路名称	接入类型	接口	
默认线路	固定 IP	WAN	Default
	动态 IP	WAN	Default
备份线路	固定 IP	WAN2(DMZ)	IPETH
	动态 IP	WAN2(DMZ)	DefaultDMZ
自定义的其他名称	固定 IP	LAN	FIXRT_01
		WAN	FIXRT_02
		WAN2(DMZ)	FIXRT_03
	动态 IP	LAN	DYNRT_01
		WAN	DYNRT_02
		WAN2(DMZ)	DYNRT_03

表 6-2 系统保留的缺省路由名

2. 检测路由

在***基本配置—>线路组合***中，当默认线路或其他某条上网线路启用线路检测后，系统还会自动生成相应的检测路由，从而保证检测包是通过当前待检测的线路转发的。可在本页面的“路由信息列表”中查看到对应路由的配置信息。不同情况下，各条上网线路对应的检测路由的名称不同，具体信息参见表 6-3。

提示：对于固定 IP 或动态 IP 接入线路来说，当“检测目标”为“网关”时，系统将直接使用该线路对应的缺省路由来检测线路，即该缺省路由同时也作为检测路由来使用。

上网线路			检测路由名
线路名称	接入类型	接口	
默认线路	任意	WAN1	Detect
备份线路	任意	WAN2(DMZ)	DetectDMZ
自定义的其他名称	固定 IP	LAN	DETEFIX _01
		WAN1	DETEFIX _02
		WAN2(DMZ)	DETEFIX _03
	动态 IP	LAN	DETEDYN _01
		WAN1	DETEDYN _02
		WAN2(DMZ)	DETEDYN _03

	PPPoE 拨号接入	此时，检测路由名与接口无关。按照配置顺序，各条 PPPoE 拨号线路对应的检测路由的名称依次为 DETEPPP _01、DETEPPP _02、DETEPPP _03、……、DETEPPP _10、DETEPPP _11、……。

表 6-3 系统保留的检测路由名

6.2.3 静态路由配置

图 6-6 静态路由配置

- 路由名：静态路由的名称（自定义，不可重复）。取值范围：1~11 个字符；
- 预定义：配置单条静态路由时，必须使用缺省值“无”。只有在配置静态路由策略库时才需修改；
- 目的网络：此静态路由的目的网络号；
- 子网掩码：此静态路由的目的网络的掩码；
- 网关地址：下一跳路由器入口的 IP 地址，设备通过接口和网关定义一条跳到下一个路由器的线路。通常情况下，接口和网关需要在同一网段；
- 绑定：指定数据包的转发接口，与该静态路由匹配的数据包将从指定接口转发。固定 IP 或动态 IP 线路对应的接口为物理接口；PPPoE 等拨号线路对应的接口为拨号接口。选项包括：
  - 各条线路的“线路名称”；
  - 各个物理接口的名称；
  - 其他内部接口。

  其中，各个内部接口含义如下：
  - Blackhole-内部接口，转发到该接口的所有包都被设备丢弃；

- Local-内部软路由接口，转发到设备本身；
- Reject-内部接口，转发到该接口的所有包都被设备拒绝，并回应一个 ICMP 不可达；
- Loopback-回环地址，代表 127.0.0.0/8 网段，不被转发。

◆ 检测间隔：同***基本配置—>线路组合***中的“检测间隔”，线路检测时发送检测包的时间间隔；

◆ 优先级：该路由的优先级，目的网段相同的情况下，设备将优先选择优先级高的路由转发数据包，值越低优先级越高；

◆ 跳数：从源到目的的路径中每一跳被赋以一个跳数值，此值通常为 1。跳数也表示该条路由记录的质量，一般情况下，如果有多条到达相同目的地的路由，设备会采用跳数值小的那条路由。

▶ 保存：静态路由配置参数生效；

▶ 重填：恢复到修改前的配置参数。

提示：

1. 配置静态路由时，必须明确下一跳地址，可通过“网关地址”或“绑定”设置。若转发接口是物理接口，则必须设置“网关地址”，但可以不设置“绑定”，此时，设备将会自动选择一条最优路径；若转发接口是拨号接口，则必须将“绑定”设置为对应的“线路名称”，但无需设置“网关地址”，此时，下一跳网关是 PPPoE 拨号所得的 IP 地址。

2. 一般情况下，请不要修改系统保留路由，以免上网异常；

3. “预定义”选项仅在 HiPER 520 产品界面上提供。

6.2.4 路由信息列表

路由信息列表
1/253
1/1 第一页 上一页 下一页 最后页 前往 第 页 搜索
路由名 预定义 目的网络 子网掩码 网关地址 检测间隔 优先级 跳数 绑定 编辑
Default 无 0.0.0.0 0.0.0.0 200.200.202.254 0 60 1 默认线路 编辑
全选 / 全不选
删除

表 6-4 路由信息列表

▶ 增加静态路由：选中“添加”选项，输入静态路由信息，单击“保存”按钮，生成新的静态路由；

- 浏览静态路由：如果已经生成了静态路由，可以查看“路由信息列表”，浏览静态路由信息；
- 编辑静态路由：如果想编辑某条静态路由，只需单击此静态路由的“路由名”或“编辑”超链接，其信息就会填充到相应的编辑框内，然后修改它，再单击“保存”按钮，修改完毕；
- 删除静态路由：选中一些静态路由，单击右下角的“删除”按钮，即可删除被选中的静态路由；

6.2.5 自定义静态路由

第一步，进入***高级配置—>路由配置***页面；

第二步，选择“添加”选项，填入静态路由的名称；

第三步，输入该条路由指向的目的网段及子网掩码；

第四步，根据实际情况，设置网关地址或者绑定的接口（注意：若转发接口是物理接口，则必须设置“网关地址”，但可以不设置“绑定”，此时设备将会自动选择一条最优路径；若转发接口是拨号接口，则必须将“绑定”设置为对应的“线路名称”，但无需设置“网关地址”）；

例如，某条路由的目的网段为 192.168.1.0/24，转发接口为物理接口，“网关地址”为 192.168.16.254，则可以不设置“绑定”，设备会自动选择路径，具体配置如下图所示。

图 6-7 静态路由配置——实例一

例如，某条静态路由的目的网段为 218.19.213.45/32，转发接口为 PPPoE 拨号接口，则必须将“绑定”设置为对应线路的“线路名称”（此处假设为“测试线路 1”），而无需设置“网关地址”，此时，其下一跳网关是 PPPoE 拨号所得的 IP 地址。具体配置如下图所示。

图 6-8 静态路由配置——实例二

第五步，如果需要监测线路状态，则需要设定检测间隔；

第六步，根据需要设置该条路由的优先级和路由跳数；

第七步，单击“保存”按钮，该静态路由添加成功。可以在“路由信息列表”中看到相应的记录；

第八步，继续配置其他静态路由。

提示：若要删除路由，只需在“路由信息列表”中选中要删除的路由，单击“删除”按钮即可。

6.3 IP/MAC 绑定

本节主要讲述***高级配置—>IP/MAC 绑定***的配置方法。

6.3.1 IP/MAC 绑定功能介绍

6.3.1.1 IP/MAC 绑定概述

要实现网络安全管理，首先必须解决用户的身份识别问题，然后才能进行必要的业务授权工作。在本节，我们将介绍如何解决用户的身份识别问题。

在设备中，通过 IP/MAC 绑定功能完成用户的身份识别工作。使用绑定的 IP/MAC 地址对作为用户唯一的身份识别标识，可以保护设备和网络不受 IP 欺骗的攻击。IP 欺骗攻击是一台主机企图使用另一台受信任的主机的 IP 地址连接到设备或者通过设备。这台电脑的 IP 地址可以轻易地改变为受信任的地址，但是 MAC 地址是由生产厂家添加到以太网卡上的，不能轻易地改变。

通过在“IP/MAC 绑定配置”中添加可信的计算机的静态 IP 地址和对应的 MAC 地址，即可在“IP/MAC 绑定信息列表”中形成对应的 IP/MAC 地址对条目。注意，在“IP/MAC 绑定信息列表”中，还可设置 IP/MAC 绑定条目的上网状态，从而控制对应的 IP/MAC 绑定用户是否可以上网。当某个 IP/MAC 绑定条目选中“允许”时（方框中出现“√”），表示上网状态为“允许”，即允许与该 IP/MAC 地址对完全匹配的用户上网；未选中“允许”时（方框中没有“√”），表示上网状态为“禁止”，即禁止与该 IP/MAC 地址对完全匹配的用户上网。

6.3.1.2 IP/MAC 绑定的工作原理

为方便起见，我们先介绍一下设备中，合法用户、非法用户及身份未知用户的概念。

合法用户：其 IP 及 MAC 地址与“IP/MAC 绑定信息列表”中的某条目的 IP 及 MAC 地址完全匹配，且该条目的“允许”被选中。

非法用户：其 IP 及 MAC 地址与“IP/MAC 绑定信息列表”中的某条目的 IP 及 MAC 地址完全匹配，且该条目的“允许” 未被选中；或者，其 IP 和 MAC 地址中有且只有一个某绑定条目的对应信息匹配。

身份未知用户：即**非 IP/MAC 绑定用户**，其 IP 或 MAC 地址均不与“IP/MAC 绑定信息列表”中的任何条目的 IP 或 MAC 地址匹配，也就是除合法用户以及非法用户之外的所有用户。

对于身份未知的用户，是在 IP/MAC 绑定全局设置中统一控制的。如果选中“允许未被 IP/MAC 绑定的主机通过”，就表示允许这些用户连接或者通过设备；如果没有选中“允许未被 IP/MAC 绑定的主机通过”，就表示禁止这些用户连接或者通过设备。

IP/MAC 绑定应用于来自于局域网内部，连接到设备的数据包或者通过设备上网的数据

包。当局域网用户有数据流量连接和通过设备时，将首先和“IP/MAC 绑定信息列表”中的条目相比较，即进行身份识别；之后，根据用户身份的不同，来自该用户的数据包将被丢弃或进入 IP 业务管理功能模块处理（即继续去匹配业务策略）。具体描述如下：

1. 如果该用户是合法用户，则允许该数据包通过，并继续去匹配业务策略；
2. 如果该用户是非法用户，则丢弃该数据包；
3. 如果该用户身份未知，则根据 IP/MAC 绑定全局配置执行：
   1) 若允许身份未知用户，即选中“允许未被 IP/MAC 绑定的主机通过”时，则允许该数据包通过，并继续去匹配业务策略；
   2) 若禁止身份未知用户，即没有选中“允许未被 IP/MAC 绑定的主机通过”时，则丢弃该数据包。

例如，如果某用户 IP/MAC 地址对 192.168.16.3 和 00:21:85:9b:45:45 已经添加到“IP/MAC 绑定信息列表”，且上网状态为“允许”（方框中出现“√”），如下表所示：

IP/MAC绑定信息列表 1/30

1/1 第一页 上一页 下一页 最后页 前往 第 页 搜索

	用户名	IP地址	MAC地址	允许上网	编辑
☐	192.168.16.3	192.168.16.3	0021859b4545	☑	编辑

☐ 全选 / 全不选 删除 GO

表 6-5 IP/MAC 绑定信息列表——实例一

那么，当设备接收到来自局域网的数据包时，将会根据以下几种情况处理：

1. 一个 IP 地址为 192.168.16.3，MAC 地址为 00:21:85:9b:45:45 的数据包将被允许通过，并继续去匹配业务策略；
2. 一个 IP 地址为 192.168.16.3，但是使用了其他 MAC 地址的数据包将立即被丢弃，以防止 IP 欺骗攻击；
3. 一个使用了其他 IP 地址，但是 MAC 地址是 00:21:85:9b:45:45 的数据包也将被丢弃，以防止 IP 欺骗攻击；
4. 如果这个数据包的 IP 地址和 MAC 地址在“IP/MAC 绑定信息列表”都没有定义：
   1） 如果选中“允许非 IP 和 MAC 绑定用户”，则允许该数据包通过，并继续去匹配业务策略。

2） 如果没有选中“允许非 IP 和 MAC 绑定用户”，则禁止该数据包通过。

如果希望禁止该用户上网，则可以直接取消“允许”的选中，即可将其上网状态改为“禁止”，如 6-5 所示。这时，IP 地址为 192.168.16.3，MAC 地址为 00:21:85:9b:45:45 的数据包将被丢弃，其他情况下设备对数据包的处理同上。

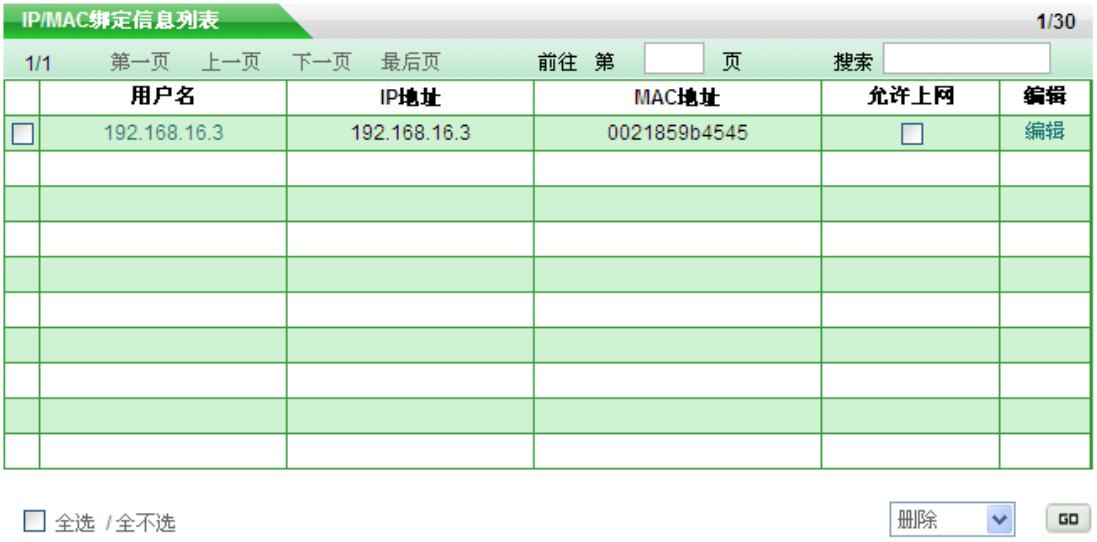


表 6-6 IP/MAC 绑定信息列表——实例二

注意，在启用了 IP/MAC 绑定功能之后，如果修改了一台电脑的 IP 地址或者 MAC 地址，而且此 IP 地址和 MAC 地址已经在“IP/MAC 绑定信息列表”中，则必须同时修改“IP/MAC 绑定信息列表”中的相应的条目。否则这台电脑将无法访问设备或者通过设备。当未选中“允许未被 IP/MAC 绑定的主机通过”时，如果希望局域网中新增的主机可以访问或通过设备，则必须为该主机在“IP/MAC 绑定信息列表”中添加 IP/MAC 绑定地址对，并选中“允许”，即允许该主机上网。

IP/MAC 绑定功能只能影响用户访问设备或通过设备访问其他网络（如 Internet），但不能影响局域网内部通信（或不经过该设备的通信）。如果用户修改了 IP 或 MAC，将有可能无法访问设备或通过设备访问其他网络（如 Internet），但是不会影响局域网内部通信，比如网络邻居浏览。

6.3.2 IP 和 MAC 绑定配置

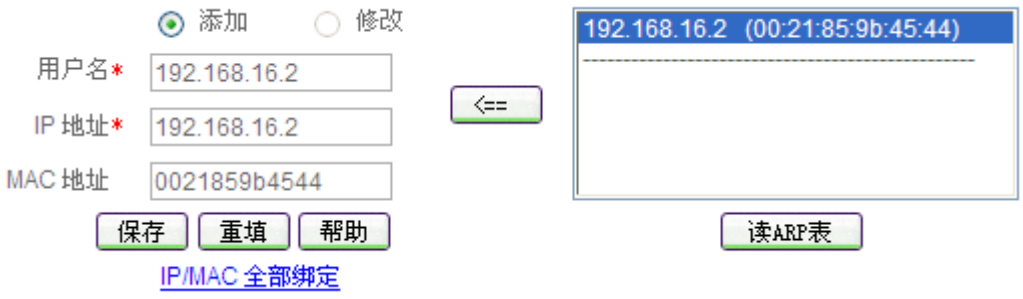


图 6-9 IP/MAC 地址绑定配置

- 用户名：欲进行 IP 和 MAC 地址绑定的用户名称。自定义，不能重复，取值范围：1～31 个字符；
- IP 地址：该用户的 IP 地址（本机的 IP 地址可使用 ipconfig /all 命令获得）；
- MAC 地址：该用户的 MAC 地址（本机的 MAC 地址可使用 ipconfig /all 命令获得）。
- 保存：IP/MAC 绑定用户配置参数生效；
- 重填：恢复到修改前的配置参数；
- 读 ARP 表：显示 LAN 口的动态 ARP 列表，即设备通过 LAN 口动态学习到的用户的 ARP 信息。注意，如果已经将某用户的 IP/MAC 地址对添加到“IP/MAC 绑定信息列表”中，该用户的 IP/MAC 地址对将不再显示。
- <==（向左箭头）：用于自动添加 IP/MAC 绑定条目。在动态 ARP 列表中，先选中一个 IP/MAC 地址对，比如 192.168.16.2（00:21:85:9b:45:44），再双击它或单击“<==”按钮，相关信息即可填充到配置框中（“用户名”也被 IP 地址填充，可修改），然后单击“保存”按钮，即可将之添加到“IP/MAC 绑定信息列表”中；
- IP/MAC 全部绑定：若希望一次性将局域网主机的 IP/MAC 地址对全部绑定，则可以直接单击“IP/MAC 全部绑定”超链接，转到 ***ARP 欺骗防御***页面，然后在“动态 ARP 表”中执行全部绑定操作。

6.3.3 IP/MAC 绑定全局配置

图 6-10 IP/MAC 绑定全局配置

- 允许未被 IP/MAC 绑定的主机通过：允许或禁止非 IP/MAC 绑定用户连接到设备。
- 保存：IP/MAC 绑定全局配置参数生效；
- 重填：恢复到修改前的配置参数；

提示：当决定取消“允许未被 IP/MAC 绑定的主机通过”功能前，必须确认管理计算机已经被添加到“IP/MAC 绑定信息列表”中，否则将会造成管理计算机无法连接到设备的现象。

6.3.4 IP/MAC 绑定信息列表

表 6-7 IP/MAC 绑定信息列表

- 查看：在“IP/MAC 绑定信息列表”中可以查看已配置绑定的用户信息，包括用户名、IP 地址、MAC 地址等信息；
- 编辑：如果想编辑某个 IP/MAC 绑定条目，只需单击该条目的“用户名”或“编辑”超链接，其信息就会填充到相应的编辑框内，可修改用户名和 MAC 地址，再单击“保存”按钮，修改完毕；如果想编辑某个 IP/MAC 绑定条目的上网状态，则只需直接单击“允许”列中的方框，即可修改。选中“允许”时，表示上网状态为“允许”，即允许与该条目完全匹配的用户上网；未选中“允许”时，表示上网状态为“禁止”，即禁止与该条目完全匹配的用户上网；
- 删除：选中一些 IP/MAC 绑定条目，在列表右下方的下拉框中选择“删除”选项，并单击“GO”按钮，即可删除被选中的条目；
- 全部删除：选中一些绑定类型为“IP/MAC”的 IP/MAC 绑定条目，在列表右下方的下拉框中选择“IP/MAC 全部删除”选项，并单击“GO”按钮，即可删除被选中的条目；

6.3.5 自定义 IP/MAC 绑定条目

配置 IP/MAC 绑定条目的步骤如下：

第一步，进入***高级配置—>IP/MAC 绑定***页面；

第二步，选择“添加”选项，输入 “用户名”（自定义）、“IP 地址”和“MAC 地址”，然后单击“保存”按钮；或者，通过动态 ARP 列表来添加用户。

第三步，该 IP/MAC 绑定条目添加成功后，可以在“IP/MAC 绑定信息列表”中查看，对于匹配该条目的数据包，将被允许连接或者通过设备。

第四步，继续配置其他 IP/MAC 绑定条目；

第五步，如果要禁止身份未知的用户连接或者是通过设备，则需取消“允许未被 IP/MAC 绑定的主机通过”的选中，然后单击“保存”按钮。否则的话，身份未知的用户也将被允许连接或者是通过设备；

第六步，如果要暂时禁止某个 IP/MAC 绑定用户上网，则可在“IP/MAC 绑定信息列表”中修改对应条目的上网状态，即取消“允许”的选中，则表示禁止与该条目完全匹配的用户上网。

当配置完 IP/MAC 绑定之后，所有发送到设备的数据包将首先和“IP/MAC 绑定信息列表”中的条目相比较。然后根据相关配置，该数据包将被丢弃或进入 IP 业务管理功能模块处理。

6.3.6 配置上网“白名单”和“黑名单”

灵活地运用 IP/MAC 绑定功能，可以为局域网用户配置上网“白名单”和“黑名单”。

通过配置上网“白名单”，将只允许“白名单”中的用户通过设备上网，禁止其他所有用户通过设备上网。因此，如果要求只允许局域网中的少数用户上网，可通过配置上网“白名单”来实现。

通过配置上网“黑名单”，将只禁止“黑名单”中的用户通过设备上网，允许其他所有用户通过设备上网。因此，如果要求只禁止局域网中的少数用户上网，可通过配置上网“黑名单”来实现。

在设备中，“白名单”中的用户即为合法用户——其 IP 及 MAC 地址与“IP/MAC 绑定信息列表”中的某条目完全匹配，且该条目选中“允许”。

“黑名单”中的用户即为非法用户——其 IP 及 MAC 地址与“IP/MAC 绑定信息列表”中的某条目完全匹配，且该条目没有选中“允许”；或者，其 IP 和 MAC 地址中有且只有一个与某个绑定条目的对应信息匹配。

6.3.6.1 配置上网“白名单”

为局域网用户配置上网“白名单”，步骤如下：

第一， 通过配置 IP/MAC 绑定条目来指定合法用户，将具有上网权限的主机的 IP 地址和 MAC 地址作为 IP/MAC 地址绑定对，并添加到“IP/MAC 绑定信息列表”中，还需选中“允许”，即允许与该 IP/MAC 地址对完全匹配的用户上网。

第二， 不选中“允许未被 IP/MAC 绑定的主机通过”，从而，其他所有不在“IP/MAC 绑定信息列表”中的主机将不能上网。

例如，如果要允许某个 IP 地址为 192.168.16.3，MAC 地址为 0022aa112233 的主机连接和通过设备，则可添加一个 IP/MAC 绑定条目，输入该主机的 IP 地址和 MAC 地址，并选中“允许”，如下表所示。

表 6-8 IP/MAC 绑定信息列表——实例三

6.3.6.2 配置上网“黑名单”

为局域网用户配置上网“黑名单”，步骤如下：

第一， 通过配置 IP/MAC 绑定条目来指定非法用户，有三种方法：

1. 将禁止上网的主机的 IP 地址和任意一个非本局域网网卡的 MAC 地址作为 IP/MAC 地址绑定对，并添加到“IP/MAC 绑定信息列表”中；
2. 将禁止上网的主机的 MAC 地址和任意一个非本局域网网段的 IP 地址作为 IP/MAC 地址绑定对，并添加到“IP/MAC 绑定信息列表”中；
3. 可将禁止上网的主机的 IP 地址和 MAC 地址作为 IP/MAC 地址绑定对，添加到“IP/MAC 绑定信息列表”中，并取消“允许”的选中（方框中无“√”），即禁止与该 IP/MAC 地址对完全匹配的用户上网。

第二， 选中“允许未被 IP/MAC 绑定的主机通过”，从而，其他所有 IP 地址和 MAC 地址均不在“IP/MAC 绑定信息列表”中的主机将能够上网。

例如，如果要禁止具有某个 MAC 地址（例如 002244002244）的主机连接和通过设备，可以添加一个 IP/MAC 地址绑定对，输入该 MAC 地址，而 IP 地址则设置成一个任意的非本局域网的 IP 地址，如下表所示。

表 6-9 IP/MAC 绑定信息列表——实例四

例如，如果要禁止具有某个 IP 地址（例如 192.168.16.100）的主机访问和连接设备，可以添加一个 IP/MAC 地址绑定对，输入该 IP 地址，而 MAC 地址则设置成任意一个非本局域网网卡的 MAC 地址，如下表所示。

表 6-10 IP/MAC 绑定信息列表——实例五

例如，如果要禁止某个 IP 地址为 192.168.16.88，MAC 地址为 0022aa112233 的主机连接和通过设备，则可添加一个 IP/MAC 地址绑定对，输入该主机的 IP 地址和 MAC 地址，并取消“允许”的选中（方框中无“√”），如下表所示。

表 6-11 IP/MAC 绑定信息列表——实例六

6.4 UPnP 配置

UPnP（Universal Plug and Play）主要用于实现设备的智能互联互通，旨在实现一种“零”配置和“隐性”的联网过程，自动发现和控制来自各家厂商的各种网络设备。

在设备上启用 UPnP 功能后，可以实现穿透 NAT：当局域网的主机通过设备与 Internet 上的终端进行通讯时，可以根据需要自动增加、删除 NAT 映射，从而保证支持 UPnP 的软件可以在 NAT 后正常使用。

通过 UPnP NAT 映射列表，可以查看经 UPnP 建立的 NAT 静态映射的相关信息，包括：内部地址、内部端口、协议、对端地址、外部端口以及信息描述。

6.4.1 启用 UPnP

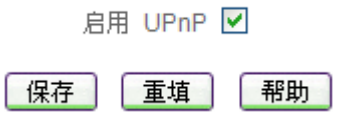


图 6-11 UPnP 配置

- 启用 UPnP：启用或者禁用 UPnP 功能，选中为启用。
- 保存：配置参数生效；
- 重填：恢复到修改前的配置参数。

提示：WEB UI 中，仅支持在 LAN 口启用 UPnP 功能。

6.4.2 UPnP NAT 映射列表

UPnP NAT映射列表
2/2
1/1 第一页 上一页 下一页 最后页 前往 第 页 搜索
序号 内部地址 内部端口 协议 对端地址 外部端口 描述
1 192.168.16.2 4173 UDP 125.39.112.92 4173 [eMule 0.48.0] [U
2 192.168.16.2 4163 TCP 0.0.0.0 4163 [eMule 0.48.0] [T
全选 / 全不选
刷新
删除

表 6-12 UPnP NAT 映射列表

表 6-13 UPnP NAT 映射列表

- 序号：该 UPnP NAT 映射的序号；
- 内部地址：局域网主机的 IP 地址；
- 内部端口：局域网主机提供的服务端口；
- 协议：该 UPnP NAT 映射使用的协议；
- 对端地址：对端主机的 IP 地址；
- 外部端口：内部端口经 NAT 转换后的端口，即设备提供给 Internet 的服务端口；
- 描述：用来描述相关 UPnP 设备厂家的信息。
- 刷新：选中“刷新”按钮，即可查看最新的 UPnP NAT 映射信息；
- 删除：选中一些 UPnP NAT 映射，单击右下角的“删除”按钮，即可删除那些被选中的 UPnP NAT 映射。

6.5 即插即用

本节主要讲述*高级配置—>即插即用*的配置方法。

6.5.1 即插即用概述

即插即用是 HIPER 500 系列产品的全新功能，在设备上启用即插即用功能后，内网用户无需更改任何网络参数设置，即无论内网用户的 IP 地址、子网掩码、网关和 DNS 服务器如何变化，都可以通过设备上网。由这种功能适合于酒店网络，故将其命名为即插即用。

6.5.2 即插即用配置

图 6-12 即插即用设置

- 启用即插即用：启用或者禁用即插即用功能，选中为启用，默认禁用此功能。启用此功能，内网用户设置任何网段的 IP 地址、网关和 DNS 地址都可以通过路由器上网。
- 保存：配置参数生效；
- 重填：恢复到修改前的配置参数。

提示：

1. 内网用户必须在本机的 TCP/IP 上进行设置网络参数，若部分参数（如网关、DNS 服务器）未填写完整，酒店即插即用功能将会无法对该主机起作用；
2. 启用即插即用功能后，系统将默认开启 ARP 代理、DNS 代理，关闭 DoS/DDoS 攻击防御；
3. 启用即插即用功能后，系统将允许未被 IP/MAC 绑定的主机通过；
4. IP 地址相同的用户不能同时上网。若一个内网用户使用某非内网 IP 地址上网，第二个使用该非法 IP 地址的用户将无法通过设备上网。
5. 内网用户的 IP 地址不能与路由器的接口（LAN 口及 WAN 口）IP 地址、路由器网关 IP 地址和路由器设置的 DNS 服务器(包括主 DNS 服务器和备 DNS 服务器)地址相同，否则将无法上网。

第7章 PPPoE 服务器

7.1 PPPoE 简介

PPPoE（Point-to-Point Protocol over Ethernet），即以太网上的点对点协议，它可以使以太网上的主机通过一个简单接入设备连到 Internet 上，并对接入的用户进行控制、计费管理。

PPPoE 协议采用 Client/Server（客户端/服务器）方式，它将 PPP 报文封装在以太网帧内，在以太网上提供点对点的连接。

7.1.1 PPPoE 连接

PPPoE 拨号连接包括 Discovery（发现）和 Session（PPP 会话）两个阶段。下面将分别介绍这两个阶段。

7.1.2 Discovery 阶段

此阶段用来建立连接，当一个用户主机想开始一个 PPPoE 会话时，首先必须进行发现阶段以识别 PPPoE Server 的以太网 MAC 地址，并建立一个 PPPoE 会话标识（Session ID）。

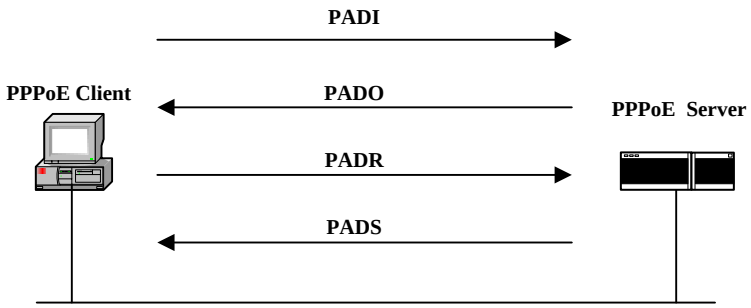


图 7-1 Discovery 阶段的基本工作流程

如上图所示， Discovery 阶段由四个步骤组成，下面将介绍它的基本工作流程。

- PADI：如果要建立一条 PPPoE 连接，首先 PPPoE 客户端就要以广播的方式发送一个 PADI(PPPoE Active Discovery Initiation)数据包，PADI 数据包包括客户端请求的服务。
- PADO：当 PPPoE 服务器收到一个 PADI 包之后，它会判断自己是否能够提供服务，如果能够提供服务的话，就会向客户端发送 PADO(PPPoE Active Discovery Offer)数据包来进行回应。PADO 数据包包括 PPPoE 服务器名称和与 PADI 数据包中相同的服务名。如果 PPPoE 服务器不能为 PADI 提供服务，则不允许用 PADO 数据包响应。

- PADR：由于 PADI 是以广播的形式发送出去的，PPPoE 客户端可能收到不止一个 PADO 数据包，它将审查所有接收到的 PADO 数据包并根据其中的服务器名或所提供的服务选择一个 PPPoE 服务器，并向选中的服务器发送 PADR（PPPoE Active Discovery Request）数据包。PADR 数据包包括客户端所请求的服务。
- PADS：当 PPPoE 服务器收到客户端发送的 PADR 包时，它就准备开始一个 PPPoE 会话，它为 PPPoE 会话创建一个唯一的 PPPoE 会话 ID，并向客户端发送 PADS (PPPoE Active Discovery Session- confirmation)包作为响应。

当发现阶段正常结束后，通信的两端都获得会话标识（Session ID）和对方的 MAC 地址，它们一起唯一定义一个 PPPoE 会话。

7.1.3 PPP 会话阶段

当 PPPoE 进入 PPP 会话阶段后，客户端和服务器将进行标准的 PPP 协商，PPP 协商通过后，数据通过 PPP 封装发送。PPP 报文作为 PPPoE 帧的净荷被封装在以太网帧内，发送到 PPPoE 链路的对端。Session ID 必须是 Discovery 阶段确定的 ID，且在会话过程中保持不变，MAC 地址必须是对端的 MAC 地址。

7.1.4 PPPoE 连接的断开

在会话阶段的任意时刻，PPPoE 服务器和客户端都可向对方发送 PADT（PPPoE Active Discovery Terminate）包通知对方结束本会话。当收到 PADT 以后，就不允许再使用该会话发送 PPP 流量了。在发送或接收到 PADT 数据包后，即使是常规的 PPP 结束数据包也不允许发送。一般情况下，PPP 通信双方使用 PPP 协议自身来结束 PPPoE 会话，但在无法使用 PPP 时可以使用 PADT 来结束会话。

7.2 PPPoE 服务器配置

HIPER 500 系列产品提供了 PPPoE 服务器的全局配置和账号配置，并可查看 PPPoE 用户的使用信息。

7.2.1 PPPoE 服务器全局配置

图 7-2 PPPoE 服务器全局配置

- 启用 PPPoE 服务器：启用/禁用设备的 PPPoE 服务器功能，选中为启用，且必须启用后才能对其中的参数进行配置；
- 起始 IP 地址：PPPoE 服务器给局域网计算机自动分配的起始 IP 地址；
- 总地址数：PPPoE 服务器可以分配的地址总数量；
- 主 DNS 服务器：PPPoE 服务器给局域网计算机自动分配的主用 DNS 服务器的 IP 地址；
- 备 DNS 服务器：PPPoE 服务器给局域网计算机自动分配的备用 DNS 服务器的 IP 地址；
- 保存：PPPoE 服务器全局配置参数生效；
- 重填：恢复到修改前的配置参数。

提示：配置了全局配置后，单击“保存”按钮，系统会提示“起始 IP 地址已经变为 **x.x.x.x**”；

7.2.2 账号配置

图 7-3 用户配置

- 用户名：用户发起 PPPoE 连接时使用的供 PPPoE 服务器验证的帐号（自定义，不可重复），取值范围：1~31 个字符；
- 密码：用户发起 PPPoE 连接时使用的供 PPPoE 服务器验证的密码；
- 描述：PPPoE 账号的描述信息；
- 保存：用户配置参数生效；
- 重填：恢复到修改前的配置参数。

7.2.3 PPPoE 用户状态信息列表

可在“PPPoE 用户状态信息列表”中查看各帐号的使用信息，如果有用户使用已配置的用户名连接到 PPPoE 服务器，我们可以在列表中看到 PPPoE 服务器为该用户分配的 IP 地址、该用户的 MAC 地址等信息。

表 7-1 PPPoE 用户状态信息列表

- 编辑：如果想编辑某一个 PPPoE 账号，只需单击它的“用户名”超链接，其信息就会填充到相应的编辑框内，修改并单击“保存”按钮即可；如果想暂时禁用某个 PPPoE 账号，同时又不删除这个账号，可在该账号的“启用”列中取消选中，当要恢复时，重新选中该选框即可；
- 删除：选中一个或多个 PPPoE 账号，单击右下角的“删除”按钮，即可删除它们；
- 挂断：先选择某条 PPPoE 会话（连接状态为“已连接”的条目），再单击“挂断”

按钮，即可挂断此 PPPoE 会话；

- 刷新：如果想查看最新的 PPPoE 账号信息，单击“刷新”按钮，及可看到最新的 PPPoE 账号的信息；

- 用户名：用户建立 PPPoE 会话使用的用户名；
- 连接状态：如果有用户使用已配置的用户名连接到 PPPoE 服务器，“连接状态”将显示“已连接”，否则显示“未连接”；
- IP 地址：PPPoE 服务器为拨入用户分配的 IP 地址；
- MAC 地址：拨入用户的 MAC 地址；
- 描述：用户配置 PPPoE 账号配置的描述信息。

7.3 PPPoE 服务器典型配置实例

1. 需求

某企业欲使用 PPPoE 接入作为内网用户的接入方式，地址池起始地址为：1.1.1.1，欲使为其内部网络配置 3 个 PPPoE 账号接入。

2. 配置步骤

1） PPPoE 全局配置

第一步，进入 ***PPPoE 服务器***页面，配置 PPPoE 全局参数；

第二步，启用 PPPoE 服务器功能，并填入相关 PPPoE 服务器全局参数，单击“保存”按钮，如下图所示：

图 7-4 PPPoE 服务器全局配置——实例

2） PPPoE 账号配置

添加 3 个 PPPoE 账号。用户名分别为 A、B 和 C，并为其配置不同的密码。账号 A 为市场部使用，描述信息配置为市场部；账号 B 配置为研发部；账号 C 配置为销售部；如下图所示。

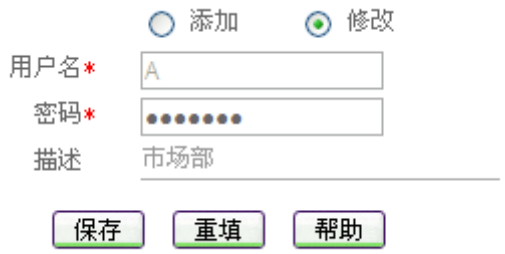


图 7-5 PPPoE 账号 A 配置——实例

图 7-6 PPPoE 账号 B 配置——实例

图 7-7 PPPoE 账号 C 配置——实例

3） 查看 PPPoE 列表

配置完成后，可通过 PPPoE 用户状态信息列表查看配置的 PPPoE 用户信息，如下图所示：

PPPoE用户状态信息列表 3/30

1/1 第一页 上一页 下一页 最后页 前往 第 页 搜索

	用户名	连接状态	IP地址	MAC地址	描述
☐	A	已连接	10.0.0.1	00:21:85:9b:45:44	
☐	B	未连接			
☐	C	未连接			

☐ 全选 / 全不选 删除 挂断 刷新

表 7-2 PPPoE 用户状态信息列表——实例

第8章 带宽管理

本章主要讲述如何对内网用户的带宽进行管理，包括配置限速规则以及查看用户信息。

8.1 带宽管理

8.1.1 带宽限速规则配置

在本页面您可以对带宽限速规则进行配置，设备提供了多条带宽限速规则配置，可根据不同的地址组为内网主机配置不同的最大上传/下载速率。

图 8-1 全局限速配置

- 地址组：用来匹配限速规则的内网 IP 地址。可引用***带宽管理—>地址组***页面设置的地址组；
- 上传速率：内网每台主机最大上传速率。单位为千比特/秒，0 表示不限制；
- 下载速率：内网每台主机最大下周速率。单位为千比特/秒，0 表示不限制。
- 保存：单击“保存”按钮，所做的配置生效；
- 重填：恢复到修改前的配置参数；
- 更多：单击“更多”前的“+”按钮，可配置更多的带宽限速。

提示：

1. HiPER 500 系列产品提供了 3 条带宽限速规则，限速规则的匹配顺序为带宽限速 3>带宽限速 2>带宽限速 1；
2. 上传速率和下载速率的单位为比特/秒（bit/s），与用户常用的软件下载单位不同，其常用的下载单位为字节/秒（Byte/s），8 比特/秒=1 字节/秒。如上图所示，当用户所设置的上传速率为 284kbit/s，下载速率为 512 kbit/s，则该用户的最大上传速度为 35.5k Byte/s，最大下载速率为 64k Byte/s。
3. 为了保证局域网用户都能正常上网，建议设置“下载速率”不低于 512Kbit/s，“上传速率”不低于 128Kbit/s。

8.1.2 用户带宽使用列表

进入*带宽管理—>带宽管理*页面，可以查看当前用户的相关信息。

表 8-1 用户带宽使用列表

- IP 地址：某用户的 IP 地址；
- 上行速率：某用户当前实时上传速率，单位：千比特/秒；
- 下行速率：某用户当前实时下载速率，单位：千比特/秒；
- 刷新：单击“刷新”按钮，可以查看“用户带宽使用列表”的最新信息。

8.1.3 带宽管理配置实例

1. 应用需求

某公司接入带宽为上行：1M bit/s，下行：4M bit/s，带机量约为 16。

要求：所有用户都要保证流畅的网络连接，对于 PPPoE 用户的限制可适量放大，对 IP 为 192.168.16.250 的用户不做带宽限制。

2. 分析

根据要求需要做三个带宽限速规则。

根据带机量、带宽以及对网络的要求，可设置每个用户的最大下行速率为 512kbit/s，上行 128 kbit/s；而对于 PPPoE 用户可配置其最大下行速率为 768 kbit/s，上行 256 kbit/s；对 IP 地址为 192.168.16.250 的用户不限速。

3. 配置步骤

配置限速规则

第一步：在*带宽管理—>地址组*中配置地址组“特殊用户”，对应 IP 地址 192.168.16.250，如下图所示：

图 8-2 特殊用户地址组配置——实例

第二步：进入***带宽管理—>带宽管理***页面，配置带宽限速 1，地址组为所有用户，上传速率 128kbit/s，下载速率为 512kbit/s。

第三步，单击带宽限速 1 的“更多”前的“+”按钮，增加带宽限速 2。配置带宽限速 2，地址组委 PPPoE 用户，上传速率 256kbit/s，下载速率为 768kbit/s。

第四步，单击带宽限速 2 的“更多”前的“+”按钮，增加带宽限速 3。配置带宽限速 3，地址组为配置的特殊用户，上传速率和下载速率不限制，设为 0。

第五步，单击“保存”按钮，完成配置，如下图所示：

图 8-3 带宽管理配置——实例

8.2 地址组

在进入*带宽管理—>带宽管理*页面和*上网行为管理—>上网行为管理*页面配置之前，必须进入本页面配置所要引用的地址组。带宽限速规则和上网行为管理策略使用地址组来匹配设备接收数据包的源地址和目的地址，在地址和时间均匹配的情况下，如果设备接收数据包的源地址和目的地址在某条带宽限速规则或上网行为管理策略的源地址组和目的地址组范围内，就对该数据包执行限速规则或执行上网行为管理策略。

用户在创建一个地址组时，可以自定义此地址组包含的 IP 地址段，也可把已有地址组添加到此地址组中。地址组可以只包含 IP 地址段或只包含其他地址组，也可以既包含 IP 地址段又包含其他地址组，但最多只能包含 10 个 IP 地址段或地址组。

中使用地址组，省掉了手工建立多条相同策略和规则的麻烦。例如，内网中有多个不连续的 IP 地址段，而这些 IP 地址段访问外网的权限又相同，可以配置这些地址段属于同一地址组，然后做一条使用此地址组的策略即可同时对它们的数据包进行控制。

8.2.1 地址组配置

图 8-4 创建地址组

- 地址组名：自定义地址组的名称，不能重复，取值范围：1~11 位字符；
- 新地址：输入欲添加到地址组中的 IP 地址段；
- 已有地址：显示已存在的地址组，可把已有地址组添加到“地址范围列表”中；
- 地址范围列表：显示地址组包含的 IP 地址段或地址组；
- “==>”：用于将自定义的 IP 地址段或已有地址组添加到“地址范围列表”中；
- “<==”：用于将“地址范围列表”中的 IP 地址段或地址组导入到“新地址”或“已有地址”框中；
- 删除：用于删除“地址范围列表”中的 IP 地址段或地址组；
- 保存：单击“保存”按钮，地址组配置参数生效；

- 重填：恢复到修改前的配置参数。

提示：

1. 地址组名称不区分大小写，即地址组“A”和“a”指的是同一个地址组，在配置时一定要注意。
2. 在配置地址组包含其它地址组时，一定要注意，如果某个地址组已经包含了其它地址组，则这个地址组不能再配置属于其它地址组。

配置地址组：首先输入自定义的地址组名并选择所属区域，然后在“新地址”配置框中输入 IP 地址段，再单击“==>”将此 IP 地址段添加到“地址范围列表”中，可连续添加多个 IP 地址段；也可在“已有地址”框中选中一个或多个地址组名，单击“==>”将已有地址组添加到“地址范围列表”中，最后单击“保存”按钮即可。

编辑地址组：如果想修改某个地址组的信息，在“地址组信息列表”中单击此地址组的“地址组名”或“编辑”超链接，其配置信息即填充到地址组配置框中，如果想修改地址组包含的 IP 地址段，在“地址范围列表”中选中此 IP 地址段，单击“<==”按钮将此 IP 地址段导入到“新地址”配置框中，修改此地址段，保存后修改成功；如果想删除某个 IP 地址段或地址组，在“地址范围列表”中选中它，单击“删除”按钮并保存后即可将其从该地址组中删除。

可在“地址组信息列表”中查看已配置的地址组信息。如下表所示。

地址组信息列表 2/100

1/1 第一页 上一页 下一页 最后页 前往 第 页 搜索

	地址组名	地址范围	编辑
☐	A	{192.168.16.50-192.168.16.52} ; {192.168.16.55-192.168.16.60 ...	编辑
☐	B	{192.168.1.20-192.168.1.25} ; {1.1.1.1-1.1.1.254} ;	编辑

☐ 全选 / 全不选 删除

表 8-2 地址组信息列表

- 编辑：如果想修改某个地址组，只需在“地址组信息列表”中单击“地址组名”或“编辑”超链接，其信息即会填充到地址组配置框内，修改并单击“保存”按钮即可；
- 删除：选中欲删除的一个或多个地址组，单击右下角的“删除”按钮，即可删除。注意：您无法删除已经在访问控制策略中引用的地址组，必须先修改或删除所有引用它的访问控制策略，才能删除此地址组。

8.3 时间段

本节主要讲述*带宽管理—>时间段*的配置方法。

提示：只有在*系统管理—>时钟管理*中，为设备设置了正确的时间后，时间段功能才能正常工作。

配置时间段，可以被某些高级功能（如拨号时间段、带宽管理以及访问控制策略等）引用，以控制这些业务的生效时间，从而达到控制上网费用、控制游戏时间等目的。

一个时间段最多可以由 8 个时间单元组成，同时还可通过参数“开始日期和时间”和“结束日期和时间”设置该时间段的生效时间。当时间段有效期已过，该时间段无效。“开始日期和时间”、“结束日期和时间”均设成 1990 年 1 月 1 日 00:00:00，代表该时间段永久有效。

8.3.1 时间段配置

图 8-5 时间段配置

图 8-6 日期设置——时间段设置

- 时间段名称：时间段策略的名称（自定义，不能重复）。取值范围：1～11 个字符；
- 开始日期、结束日期：该时间段策略生效的开始和结束的日期。开始日期和结束日期可以通过 2 种方式进行设置：日期输入范围为 1989-1-1 到 2050-12-31。
  - 直接输入。通过直接输入 YYYY-MM-DD 的格式，YYYY 代表年份，MM 代表月份， DD 表示日期。如 2009-03-23（或 2009-3-23）表示 2009 年 3 月 23 日。
  - 下拉日历选择。如图 8-6 所示，通过日历控件直接选择开始或结束日期。单击“<年”、“年>”选择年份；单击“<月”、“月>”选择月份；在日历中直接单击所要选择的日期。
- 时间单元一～时间单元八：该时间段要控制的时间单元，一个时间段最多可由 8 个时间单元组成；
- 类型：时间单元的类型，类型有每天、星期一、星期二、……、星期日、工作日（周一至周五）、周末（周六、周日）等；
- 开始时间：每个时间单元的开始时间，系统默认为 00:00:00（单位：时:分:秒）；
- 结束时间：每个时间单元的结束时间，系统默认为 23:59:59（单位：时:分:秒）；
- 保存：时间段配置参数生效；
- 重填：恢复到修改前的配置参数。

提示：一个跨越零点的连续时间段，必须配置成两个连续的时间单元，例如，从晚上 8 点到次日凌晨 5 点需要以 24:00:00 分为两个时间段，即第一个时间单元为 20:00:00～23:59:59，第二个时间单元为 00:00:00～05:00:00。

8.3.2 时间段列表

表 8-3 时间段信息列表

- 增加时间段：选中“添加”选项，输入时间段信息，单击“保存”按钮，生成新的时间段；
- 浏览时间段：如果已经配置了时间段，可在“时间段信息列表”中浏览相关信息，如上表所示；
- 编辑时间段：如果想编辑某一时间段，只需单击此时间段条目中的“时间段名称”或“编辑”超链接，其信息就会填充到相应的编辑框内，可修改它，再单击“保存”按钮，修改完毕；
- 删除时间段：选中一些时间段，单击右下角的“删除”按钮，即可删除被选中的时间段；
- 查看时间段详细信息：单击某个时间段条目中的“详细”超链接，可显示该时间段的详细信息，以及被其他功能引用的相关信息，如下图所示。

图 8-7 时间段详细信息

8.3.3 自定义时间段

第一步，进入*带宽管理—>时间段*页面；

第二步，单击“添加”按钮，填写时间段名称；

第三步，根据需要填写该时间段的起止时间；

第四步，填写时间段具体时间单元信息；

第五步，单击“保存”按钮，时间段配置完成，可在“时间段信息列表”中看到添加的记录；

第六步，继续添加新的时间段信息。

提示：若要删除时间段，只需在“时间段信息列表”中选中要删除的时间段，单击“删除”按钮，即可删除。

8.3.4 时间段配置实例

1. 应用需求

2010 年度某公司为控制销售部门员工的上网行为，针对其实际需求，规定在工作时间中只允许 WEB 业务，在其余时间则开放所有业务。该公司的工作时间为：周一～周五，上午 9 点～12 点，下午 1 点～6 点；中午 12 点～13 点为午间休息时间。

2. 分析

由上，可以将该公司上网时间划分为工作时间（worktime）和休息时间（freetime）两个时间段。

1) 工作时间段划分为 2 个时间单元，具体信息如下：

开始日期：2010 年 1 月 1 日

结束日期：2010 年 12 月 31 日

时间单元一：类型为“工作日（周一至周五）”，开始时间 09:00:00，结束时间 11:59:59

时间单元二：类型为“工作日（周一至周五）”，开始时间 13:00:00，结束时间 17:59:59

2) 由于休息时间段划分为 4 个时间单元，具体信息如下：

开始日期：2010 年 1 月 1 日

结束日期：2010 年 12 月 31 日

时间单元一：类型为“工作日（周一至周五）”，开始时间 00:00:00，结束时间 08:59:59

时间单元二：类型为“工作日（周一至周五）”，开始时间 12:00:00，结束时间 12:59:59

时间单元三：类型为“工作日（周一至周五）”，开始时间 18:00:00，结束时间 23:59:59

时间单元四：类型为“周末（周六、周日）”，开始时间 00:00:00，结束时间 23:59:59

3. 配置步骤

第一步，进入***带宽管理—>时间段***页面；

第二步，配置工作时间段“worktime”。选中“添加”选项，在“时间段名称”中填入 worktime；

第三步，设置 worktime 起止时间：

在“开始日期”中填入 2010-1-1；

在“结束日期”中填入 2010-12-31；

第四步，分别设置该时间段的 2 个时间单元，首先选择类型，然后填入开始时间和结束时间：

时间单元一：在“类型”中选择“工作日（周一至周五）”，在“开始时间”中填入 09:00:00，

在“结束时间”中填入 11:59:59；

时间单元二：在“类型”中选择“工作日（周一至周五）”，在“开始时间”中填入 13:00:00，在“结束时间”中填入 17:59:59；

第五步，单击“保存”按钮，时间段“worktime”设置成功，如图 8-8 所示：

图 8-8 时间段 worktime 配置——实例

第六步，配置休息时间段“freetime”。选中“添加”选项，如下图所示，在“时间段名称”中填入 freetime；

第七步，设置 freetime 起止时间：

在“开始日期”中填入 2008-1-1；

在“结束日期”中填入 2008-12-31；

第八步，分别设置该时间段的 4 个工作单元，首先选择类型，然后填入开始时间和结束时间。

时间单元一：在“类型”中选择“工作日（周一至周五）”，在“开始时间”中填入 00:00:00，在“结束时间”中填入 08:59:59；

时间单元二：在“类型”中选择“工作日（周一至周五）”，在“开始时间”中填入 12:00:00，在“结束时间”中填入 12:59:59；

时间单元三：在“类型”中选择“工作日（周一至周五）”，在“开始时间”中填入 18:00:00，在“结束时间”中填入 23:59:59；

时间单元四：在“类型”中选择“周末（周六、周日）”，在“开始时间”中填入 00:00:00，在“结束时间”中填入 23:59:59；

第九步，单击“保存”按钮，时间段“freetime”设置成功，如图 8-9 所示。

图 8-9 时间段 freetime 配置——实例

至此，时间段“worktime”和“freetime”配置成功，可在“时间段信息列表”中查看、编辑它们。

第9章 上网行为管理

9.1 上网行为管理

本节主要讲述*上网行为管理—>上网行为管理*的配置及使用方法。

在本页面可以设置对指定局域网地址组用户的上网行为进行管理，包括禁止局域网用户使用即时聊天软件 QQ、MSN 进行聊天，禁止局域网用户使用 BitComet 或比特精灵进行 BT 下载；禁止讯雷搜索资源；禁止局域网用户使用 HTTP 下载扩展名为 exe、dll、vbs、bat、com、sys 的文件，禁止局域网用户在网页上提交输入；禁止局域网用户使用 QQ 游戏等网络游戏软件；禁止局域网用户访问特定的股票网址和游戏网址；禁止局域网用户使用 HTTP 代理等功能。

9.1.1 上网行为管理配置

进入*上网行为管理—>上网行为管理*页面，对局域网用户的上网行为进行管理和控制，可配置以下参数：

- 地址组：该上网行为管理策略的生效地址组，引用*带宽管理—>地址组*中所配置的地址组。
- IM 过滤：对局域网用户使用即时通讯软件（Instant Message）进行控制，包括：
  - QQ：禁止或允许局域网用户进行 QQ 聊天，选中表示禁止；
  - MSN：禁止或允许局域网用户进行 MSN 聊天，选中表示禁止；
  - Ali：禁止或允许局域网用户登录阿里巴巴软件，选中表示禁止；
  - WebQQ：禁止或允许局域网用户使用网页 QQ 聊天，选中表示禁止；
  - Fetion：禁止或允许局域网用户进行飞信聊天，选中表示禁止。
- P2P 过滤：对局域网用户使用 P2P 软件进行过滤控制，包括：
  - BT：禁止或允许局域网用户进行 BitComet、比特精灵下载，选中表示禁止；
  - Thunder：禁止或允许局域网用户进行讯雷搜索资源，选中表示禁止；
  - QQLive：禁止或允许局域网用户使用 QQLive 播放视频，选中表示禁止；
  - PPStream：禁止或允许局域网用户使用 PPStream 播放视频，选中表示禁止；
  - Kugoo：禁止或允许局域网用户使用 Kugoo 播放视频，选中表示禁止；
  - PPLIVE：禁止或允许局域网用户使用 PPLIVE 播放视频，选中表示禁止；
  - qvod：禁止或允许局域网用户使用 qvod 播放视频，选中表示禁止。
- 游戏过滤：对局域网用户使用的网络游戏软件进行控制，包括
  - QQGame：禁止或允许局域网用户使用 QQ 游戏，选中表示禁止；
  - PaoPao：禁止或允许局域网用户使用泡泡堂游戏，选中表示禁止；

- zhengtu：禁止或允许局域网用户使用征途游戏，选中表示禁止；
- wanmei：禁止或允许局域网用户使用完美世界、诛仙，选中表示禁止；
- xiyou：禁止或允许局域网用户使用梦幻西游，选中表示禁止；
- jwt：禁止或允许局域网用户使用劲舞团，选中表示禁止；
- HFang：禁止或允许局域网用户使用浩方，选中表示禁止；
- WOW：禁止或允许局域网用户使用魔兽世界，选中表示禁止；
- AION：禁止或允许局域网用户使用永恒之塔，选中表示禁止；
- popCar：禁止或允许局域网用户使用跑跑卡丁车，选中表示禁止。

◆ 网页元素过滤：对局域网用户使用浏览器访问网页的元素进行控制，包括：

- FileType：禁止或允许局域网用户使用 HTTP 下载扩展名为 exe、dll、vbs、bat、com 和 sys 的文件，选中表示禁止，单击“过滤文件类型”超链接查看过滤文件类型的详细信息；
- Upload：禁止或允许当前用户在网页上提交任何输入，包括用户登录、在论坛上发表言论等选中表示禁止。。

◆ DNS 过滤：对局域网用户使用浏览器访问的域名进行控制，包括：

- GAMEURL：禁止或允许局域网用户访问特定的游戏网站，选中表示禁止，单击“游戏网站”超链接查看所有过滤的游戏网站；
- STOCKURL：禁止或允许局域网用户访问特定的证券网站，选中表示禁止，单击“股票网站”超链接查看所有过滤的股票网站。

◆ 其他过滤：对局域网用户的其他行为进行控制，包括：

- HttpProxy：禁止或允许局域网用户使用 HTTP 代理功能，选中表示禁止；
- SOCKS4：禁止或允许局域网用户使用 SOCKS4 代理功能，选中表示禁止；
- SOCKS5：禁止或允许局域网用户使用 SOCKS5 代理功能，选中表示禁止。

◆ 生效时段：选择上述策略生效的时间段，选择为空表示对所有时间段生效；时间段可在***带宽管理—>时间段***页面进行配置；

◆ 描述：上网行为管理策略的描述。

▶ 更新策略：更新对应功能的策略库，单击“更新策略”超链接，系统立即连接到指定 WEB 站点，下载并自动更新对应的策略库；

▶ 保存：上网行为管理配置参数生效；

▶ 重填：恢复到修改前的配置参数。

图 9-1 上网行为管理设置

提示：

1. 当配置了只允许 web 上网功能，只允许 web 访问功能优先；

2. 当所配置的策略的某功能不生效时，请确定该功能的策略库为最新，单击“更新策略”超链接可更新该配置的策略库；

3. 当某一内网地址可匹配多条上网行为管理策略时，匹配顺序为后进先出，即后配置的上网行为管理策略先匹配。

9.1.2 上网行为管理列表

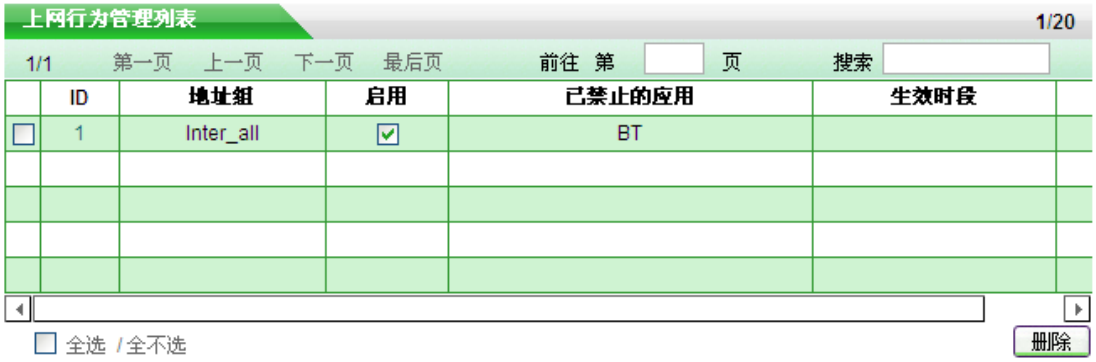


表 9-1 上网行为管理列表

表 9-2 上网行为管理（续表 9-1）

- 浏览上网行为管理策略：如果已经配置了上网行为管理策略，可在“上网行为管理列表”中浏览相关信息，如上表所示；
- 编辑上网行为管理策略：如果想编辑某一上网行为管理策略，只需单击此策略中的“ID”超链接，其信息就会填充到相应的编辑框内，可修改它，再单击“保存”按钮，修改完毕；如果想编辑某个上网行为管理策略的状态，则只需直接单击“启用”列中的方框，即可修改。选中“启用”时，表示该上网行为管理策略状态为启用，即该策略生效；未选中“启用”时，表示该上网行为管理策略状态为禁用，即该策略不生效；
- 删除上网行为管理策略：选中一些策略，单击右下角的“删除”按钮，即可删除被选中的上网行为管理策略；

9.1.3 只允许 web 访问

在上网行为管理页面，还可以配置“只允许 web 访问”功能。启用此功能，符合地址组的内网用户将只能通过 TCP 的 80 端口访问网络，其他应用将全面被禁止。

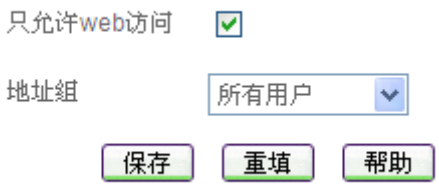


图 9-2 只允许 Web 访问

- 只允许 web 访问：启用或禁用只允许 web 访问功能，打勾表示启用；
- 地址组：只允许 web 访问引用的生效地址组，引用***带宽管理—>地址组***中所配置的地址组。
- 保存：上网行为管理配置参数生效；
- 重填：恢复到修改前的配置参数。

提示： 只允许 web 访问策略的优先级高于上网行为管理策略。当启用了只允许 web 访问后，匹配地址组的内网用户将直接匹配只允许 web 访问策略，所配置的上网行为管理策略将失效；

9.1.4 上网行为管理配置实例

1. 应用需求

2009 年度某公司为控制公司员工的上网行为，针对其实际需求，规定在工作时间中禁止所有 IM、P2P 和游戏软件，并禁止员工在上班时间查看股票及游戏网站信息。在其余时间则开放所有业务。

销售部地址为 192.168.16.50~192.168.16.70，由于工作需要，需使用即时通信软件（IM）与客户进行沟通；

其中对于部分用户（地址为 192.168.16.4 和 192.168.16.5），只允许其使用 web 访问

该公司的工作时间为：周一～周五，上午 9 点～12 点，下午 1 点～6 点。

2. 分析

由上，可以根据将该公司的上网行为管理需求，配置 2 条上网行为管理策略，并对例外部分用户进行配置。

1) 策略 1，禁止全部用户的 IM、P2P、游戏以及游戏和股票网站过滤；

2) 策略 2，禁止销售部地址段的员工 P2P、游戏以及游戏和股票网站功能，但开启 IM 软件功能；

3) 配置只允许 web 访问，为 IP 地址为 192.168.16.4 和 192.168.16.5 的用户配置一个特殊的策略；

3. 配置步骤

进入*上网行为管理—>上网行为管理*进行配置前，需要先进入*带宽管理—>地址组*配置 2 个地址段，地址段“sales”和“specila”，“sales”地址段为销售部所使用的地址，“special”地址段为 192.168.16.4~192.168.16.5；还需要进入*带宽管理—>时间段*，配置工作时间 worktime， 此处不再列出配置方法，

第一步，进入*上网行为管理—>上网行为管理*页面。

第二步，配置上网行为管理策略 1，策略名为“All”，引用设备预设的地址组“所有用户”和已设置的时间段“worktime”，禁止 IM、P2P、游戏过滤和 DNS 过滤中的功能，单击“保存”按钮，完成策略 1 的配置，如图 9-3 所示；

第三步，配置上网行为管理策略 2，策略名为“Sales”，引用地址组“Sales 和时间段“worktime”，允许 IM 软件，禁止 P2P、游戏过滤和 DNS 过滤中的功能，单击“保存”按钮，完成策略 2 的配置，如图 9-4 所示；

第四步，启用“只允许 Web 访问”功能，引用地址段位“special”，单击“保存”按钮，完成只能允许 Web 访问功能的配置，如图 9-5 所示。

配置图片如下：

图 9-3 上网行为管理实例配置——策略 1

添加
修改
地址组
sales
QQ[更新策略]
禁止QQ
MSN[更新策略]
禁止MSN
AliWW[更新策略]
禁止阿里旺旺登陆
Web_QQ[更新策略]
禁止网页QQ
FeiXin[更新策略]
禁止飞信
BT[更新策略]
禁止比特彗星, 比特精灵
Thunder[更新策略]
禁止迅雷搜索资源
QQ_Live[更新策略]
禁止QQLive
PP_Stream[更新策略]
禁止ppstream播放视频
KuGou[更新策略]
禁止酷狗音乐搜索资源
PPLIVE[更新策略]
禁止pplive播放视频
qvod[更新策略]
禁止快播
QQ_Game[更新策略]
禁止QQGame
PaoPao[更新策略]
禁止泡泡堂游戏
zhengtu[更新策略]
禁止征途游戏
wanmei[更新策略]
禁止完美世界，诛仙游戏
xiyou[更新策略]
禁止梦幻西游游戏
jwt[更新策略]
禁止劲舞团游戏
HFang[更新策略]
禁止进入浩方
WOW[更新策略]
禁止魔兽世界游戏
AION[更新策略]
禁止永恒之塔游戏
popCar[更新策略]
禁止跑跑卡丁车游戏
FileType[更新策略]
过滤文件类型
upload[更新策略]
禁止用户在网页上提交输入
GAMEURL[更新策略]
游戏网站
STOCKURL[更新策略]
证券网站
HttpProxy[更新策略]
禁止http代理
Socks_4[更新策略]
禁止SOCKS4代理
Socks_5[更新策略]
禁止SOCKS5代理
生效时段
worktime
描述
销售部允许IM
保存
重填
帮助

图 9-4 上网行为管理实例配置——策略 2

图 9-5 上网行为管理实例配置——策略 3

9.2 域名过滤

本节主要讲述*上网行为管理>域名过滤*的配置及使用方法。

9.2.1 域名过滤配置

通过在本页面进行简单的配置，可以实现禁止内网用户对某些指定域名的访问。下面将介绍如何配置域名过滤。

图 9-6 域名过滤配置

- 域名名称：自定义禁止内网用户访问的域名，不可重复，取值范围：1~63 个字符；
- 域名列表：显示用户添加的域名名称，允许/禁止内网所有用户访问这些域名；
- 添加：输入域名名称后，单击“添加”按钮，即可将输入的域名添加到“域名列表”中，可添加 100 个域名；
- 删除：在“域名列表”中选中一条或多条域名，单击“删除”按钮，即可删除选中的域名；
- 全部删除：单击“全部删除”按钮，即可将“域名列表”中的域名全部删除。

提示：

1. 设备中支持设置 100 个域名过滤；
2. 域名过滤功能是全字匹配的，当内网用户在浏览器里输入的域名与“域名列表”中显示的域名全字匹配时，将无法访问此域名对应的网页。
3. 可以在域名名称中输入通配符“*”来实现对多个域名的过滤，例如在域名列表中输入域名名称“www.163.*”，内网用户将不能访问以“www.163.”开头的所有网页。

9.2.2 域名过滤全局配置

必须启用域名过滤功能后，配置的域名过滤才生效。

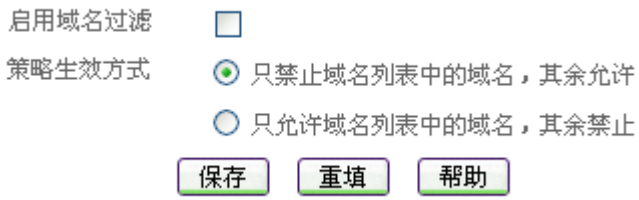


图 9-7 域名过滤全局配置

- 启用域名过滤：打勾表示启用，启用域名过滤功能后，配置的域名过滤才生效；
- 只禁止域名列表中的域名，其余允许：禁止内网用户访问列表中的域名，不在列表中的域名则可以访问；
- 只允许域名列表中的域名，其余禁止：只允许内网用户访问列表中的域名，不在列表中的域名禁止访问。
- 保存：域名过滤全局配置参数生效；
- 重填：恢复到修改前的配置参数；

9.3 策略库

本节主要讲述*上网行为管理—>策略库*的配置及使用方法。

9.3.1 策略库概述

在本页面，不仅可以查看各个策略库实例的相关信息，还允许加载、更新策略库。通过引入策略库，将复杂的多条策略当作一个策略库处理，并且可以直接通过 Internet 在线更新某个策略库或全部策略库，大大方便了用户的使用。目前，系统提供四种类型的策略库：路由策略库、DNS 策略库、网站策略库和防火墙策略库。以后，根据用户实际需求，艾泰科技将会陆续提供更多策略库。

路由策略库在*高级配置—>路由配置*中配置和引用，通过引入路由策略库，使用户无需一条条地添加静态路由，只需操作一次，就能批量配置大量电信路由或者网通路由，从而保证电信流量走电信线路、网通流量走网通线路。

防火墙策略库、DNS 策略库和网站策略库在*上网行为管理—>上网行为管理*中配置和引用，通过引入防火墙策略库，使用户无需设置大量业务策略，只需一键操作，就可实现禁止或允许局域网用户使用 QQ/MSN/BT 等业务了。

9.3.2 策略库信息列表

策略库信息列表
32/57
1/4 第一页 上一页 下一页 最后页 前往 第 页 搜索
名称 类型 说明 引用状态 版本号 更新策略
CNC 路由 网通静态路由 未引用 090805 更新
TEL 路由 电信静态路由 未引用 090805 更新
QQ 防火墙 禁止QQ 未引用 090805 更新
MSN 防火墙 禁止MSN 未引用 090805 更新
BT 防火墙 禁止比特彗星,比特精灵 未引用 090805 更新
Thunder 防火墙 禁止迅雷搜索资源 未引用 090805 更新
GAMEURL Dns 游戏网站 未引用 090805 更新
STOCKURL Dns 证券网站 未引用 090805 更新
FileType 网站 过滤文件类型 未引用 090805 更新
upload 网站 禁止用户在网页上提交输入 未引用 090805 更新
全选 /全不选
更新全部策略
删除

表 9-3 策略库信息列表

- 名称：该策略库的名称；
- 类型：该策略库的类型。目前，系统提供“防火墙”、“路由”、“DNS”和“网站”4 种类型的策略库；
- 说明：用于说明该策略库的作用；

- 引用状态：该策略库是否被引用。如果被引用，则显示为“已引用”，反之，则显示为“未引用”；
- 版本号：该策略库的版本号，版本号是根据策略库的创建日期生成的，例如 090805 就表示当前版本是 2009 年 8 月 5 号创建的。可以通过版本号来判断该策略库是否需要更新，版本号越大，就表示版本越新。
- 更新：单击某条策略库的“更新”超链接后，系统立即连接到指定 WEB 站点，下载并自动更新该策略库；
- 更新全部策略：单击“更新全部策略”超链接后，系统立即连接到指定 WEB 站点，下载并自动更新“策略库信息列表”中的全部策略库；
- 删除：首先选中一些策略库条目，再单击右下角的“删除”按钮，即可删除被选中的策略库；
- 加载：用户可以加载自定义的策略库文件。

提示：

1. 仅系统提供的缺省策略库支持“更新”和“更新全部策略”操作；

2. 缺省情况下，策略库信息列表中只显示系统默认的策略库，包括 CNC、TEL、QQ、MSN、BT、Thunder、GAMEURL、STOCKURL、FileType 等策略信息。用户也可以在命令行中自定义防火墙策略库，也可以修改系统默认防火墙策略库。

3. 当成功更新了某条被引用的策略库之后，若该策略库为防火墙策略库，则配置立即生效。若该策略库为路由策略库，则必须进入***高级配置—>路由配置***页面，重新引用并保存之后，配置才能生效；

4. 禁止删除系统提供的缺省策略库。

9.3.3 策略库版本检查

图 9-8 策略库版本检查

- 策略库版本检查：
  自动检查：系统会在指定时刻触发一次策略库版本检查，此处主要记录经检查需要更新的策略库；
  不检查：系统不再主动检查策略库版本。
- 检查时间：当“策略库版本检查”设置为“自动检查”时，可以在这里设置策略库版本检查的触发时刻。
- 保存：配置参数生效；
- 重填：恢复到修改前的配置参数。

提示：当“策略库版本检查”设置为“自动检查”时，为保证相关功能工作正常，

必须在*系统管理—>时钟管理*中准确地设置设备的时钟，使其与当地标准时间同步。

9.3.4 导入策略库

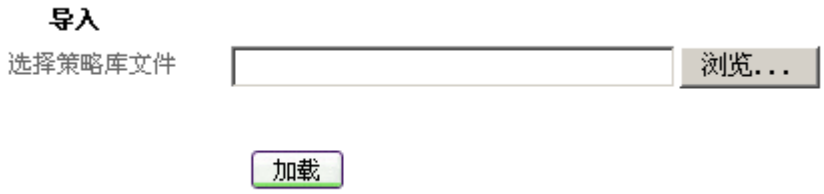


图 9-9 导入策略库

- 选择策略库文件：可在此输入策略库文件在本地计算机存放的路径，也可直接单击“浏览”按钮选择配置文件。
- 加载：首先在“选择策略库文件”中选择欲加载的策略库文件，再单击“加载”按钮，就可以将该策略库文件加载到设备中；同时，还会在“策略库信息列表”中增加该策略库的相关记录。

提示：在加载策略库文件的过程中请不要关闭设备电源，以避免不可预期的错误。

第10章 系统管理

在系统管理中，主要设置设备相关管理参数，包括管理员配置、时钟管理、软件升级、配置管理以及远程管理等等。

10.1 管理员配置

本节主要讲述***系统管理—>管理员配置***的配置方法，如图 10-1 所示。

图 10-1 管理员配置

- 管理员用户名：新 WEB 管理员的用户名。自定义，不能重复。取值范围：1～31 个字符；
- 密码：该管理员的登录密码；
- 确认密码：该管理员的登录密码，此处必须和上一栏所填密码一致；
- 保存：管理员配置参数生效；
- 重填：恢复到修改前的配置参数。
- **提示**：为安全起见，强烈建议修改初始的管理员密码，并谨慎保管管理员用户名及密码。

10.2 时钟管理

本节主要讲述***系统管理—>时钟管理***的配置，如图 10-2 所示。

为了保证设备各种涉及到时间的功能（如 DDNS 服务、时间段配置等）正常工作，需要准确地设定设备的时钟，使其与当地标准时间同步。

设备提供“手工设置时间”或者“网络时间同步”这两种设置系统时间的方式，不过，每次只能选择其中的一种方式来设置时间。

产品没有时间保存功能，设备重启后时间会恢复到出厂值，请使用“网络时间同步”功能来从互联网上获取标准的时间，当下次开机连接到 Internet 后，设备将会自动获得标准的时间。

图 10-2 时钟管理配置

- 当前系统时间：显示当前设备时钟（单位：年:月:日，时:分:秒）；
- 时区选择：选择设备所在地的国际时区，只有选择了正确的时区，网络时间同步（sntp）功能才能正常工作；
- 手工设置时间：手工输入当前的日期和时间（单位：年:月:日，时:分:秒）；
- 网络时间同步（sntp）：使用网络时间同步功能，设置了正确的 sntp 服务器后，当设备连接到 Internet 之后，就会自动和所设置 sntp 服务器同步时间。系统缺省预设两个 sntp 服务器 192.43.244.18、129.6.15.28，一般情况下不需要修改。若需更多 sntp 知识及服务器，可访问 http://www.ntp.org。
- 保存：时钟管理配置参数生效；
- 重填：恢复到修改前的配置参数。

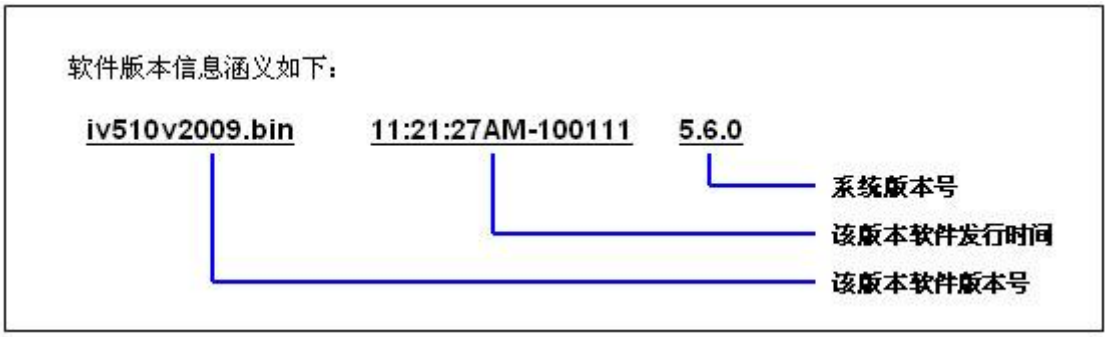
10.3 软件升级

本节主要讲述*系统管理—>软件升级*的配置方法。

10.3.1 显示和保存当前运行软件

图 10-3 显示和保存当前软件

软件版本信息涵义如下：



10.3.2 软件升级

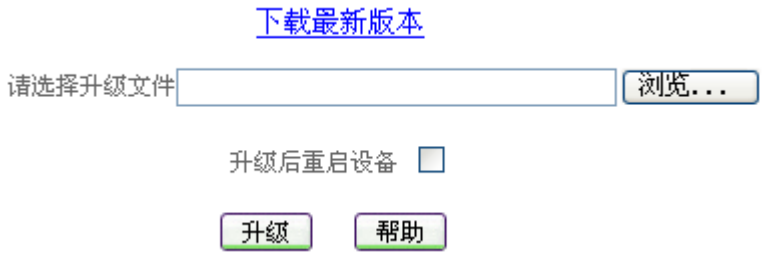


图 10-4 软件升级

第一步 下载最新软件

单击“下载最新版本”超链接，到上海艾泰科技公司官方网站下载最新的软件版本到本地计算机。

提示：请选择合适型号的最新软件；下载的软件适用的硬件平台必须和当前产品的硬件平台一致，软件版本必须比当前使用的软件版本新；

第二步　选择升级软件所在路径

在“请选择升级文件”文本框中输入将要升级的软件在本地计算机的路径，或者是通过“浏览”在本地计算机选择新软件。

- 升级后重启设备：升级软件成功之后，必须重启设备，新软件才能生效。可以选中“升级后重启设备”，设备将在软件升级成功后自动重启。如果没有选中“升级后重启设备”，请在升级成功后选择合适的时间重启设备。

第三步　更新设备的软件

单击“升级”按钮，更新设备的软件。

提示：

1. 强烈建议在设备负载比较轻（用户比较少）的情况下升级；

2. 定期的升级设备的软件，可以使设备获得更多的功能或者更佳的工作性能。正确的软件升级并不会改变当前设备设置；

3. 升级过程不能关闭设备电源，否则将会导致不可预期的错误甚至不可恢复的硬件损坏；

10.4 配置管理

本节主要讲述***系统管理—>配置管理***的配置方法。

10.4.1 恢复出厂配置

图 10-5 恢复出厂配置

- 恢复：将设备的配置恢复到出厂时的设置值。

提示：

1. 这是一个非常危险的操作，它将删除所有自定义的配置，并将系统恢复到原始状态。

2. 设备的出厂管理员用户名为：Default、默认密码为空；默认 LAN 口 IP 地址/子网掩码为：192.168.16.1/ 255.255.255.0。执行恢复出厂配置之后，建议重启设备。

10.4.2 重新启动设备

“重启设备”超链接位于二级菜单栏的最右边，在任何页面都可通过单击“重启设备”超链接来重新启动设备，在图 10-6 中可以看到 “重启设备”在页面中的位置。

图 10-6 重启设备

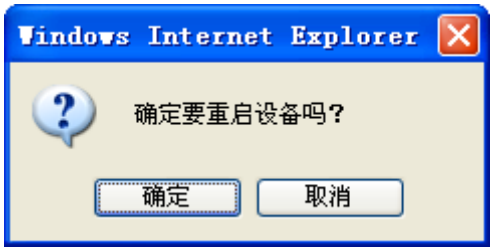


图 10-7 提示信息

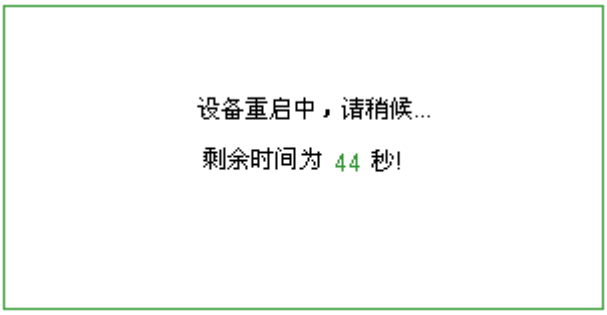


图 10-8 设备重启中

提示：

1. 鼠标指向“重启设备”超链接时，会出现“单击重启设备”的提示信息，单击“重启设备”超链接，系统会给出图 10-7 所示的提示信息，单击“确定”按钮，设备就开始了重启过程，如图 10-8 所示，设备重启需要 44 秒的时间；
2. 重启时，所有用户都将断开到设备的连接，请谨慎使用此功能；
3. 设备重启后返回到首页。

10.5 远程管理

本节主要讲述***系统管理—>远程管理***的配置方法。

由于设备内置了防火墙，将会屏蔽所有来自 Internet 的连接。如果要从 Internet 远程管理设备，必须启用相关的远程管理功能。

图 10-9 远程管理

- HTTP：允许或禁止从 Internet 通过 WEB 管理设备，设备默认外部 WEB 管理端口为 8081 。如要从 Internet 通过 WEB 管理设备必须用“IP 地址：端口”的方式（例如 http://218.21.31.3:8081）才能登录设备；
- 外部端口：可以修改设备默认外部端口（默认值为 8081）。注意，这个端口修改成 80 以后，在***高级配置—>端口映射和虚拟服务器***的“端口映射列表”中，就会增加一条 TCP80 端口的映射，此时如需要再次增加局域网 WEB 服务器的映射，就会引起冲突。
- 保存：远程管理配置参数生效；
- 重填：恢复到修改前的配置参数。

提示：

1. 设备的 Internet 地址可以从***基本配置—>线路配置***的“线路连接信息列表”中获得；

2. 为安全起见，如非必要，请不要启用 Internet 远程管理功能；在启用 Internet 远程管理功能之前，请先到***系统管理—>管理员配置***中修改设备默认密码；

3. 如果“默认线路”采用了 PPPoE 拨号，其 IP 地址是动态的，可以在***基本配置—>DDNS 配置***中配置 DDNS 功能；

4. 打开了 HTTP 管理功能之后，系统会自动生成 TCP:8081 端口的端口映射（可在***高级配置—>端口映射和虚拟服务器***的“端口映射列表”查看）；

5. 在寻求艾泰科技客服工程师服务之前，请事先打开相关远程管理功能。

10.6 系统信息

本节讲述***系统状态—>系统信息***的使用，主要包括系统版本、系统运行时间、系统告警信息等。

10.6.1 页面刷新功能

图 10-10 页面刷新功能配置

- 下拉框：用于设置采用手动或自动刷新本页面及相关页面。

  手动刷新：表示不启用自动刷新功能，只能通过单击“刷新”按钮手动刷新本页面；

  自动刷新/10 秒、自动刷新/30 秒或者自动刷新/60 秒：表示启用自动刷新功能，本页面和***系统状态—>NAT 统计***页面将每隔指定的时间间隔自动刷新。

- 刷新：单击“刷新”按钮，可查看本页面最新信息。

提示：若修改了下拉框的值，只有在单击“刷新”按钮之后，修改的配置才能被保存并生效。

10.6.2 系统运行时间

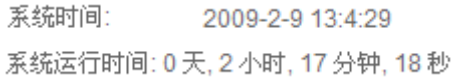


图 10-11 系统运行时间

- 系统时间：显示设备当前的日期和时间；
- 系统运行时间：显示设备本次启动至查看时刻的时间。

10.6.3 系统资源状态

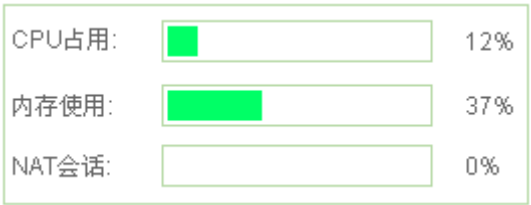


图 10-12 系统资源状态

- CPU 占用：显示当前 CPU 占用的百分比；
- 内存使用：显示当前内存使用的百分比；
- NAT 会话：显示当前建立的 NAT 会话数占设备所能处理的最大 NAT 会话数的百分比。

提示：

3. 上述三个参数的值都通过进度条和数值（百分比）两种方式显示，数值的取值范围为 0%~100%；根据数值的大小，进度条可能会显示为空、绿色、黄色或者红色：

- 当数值＜1%时，进度条为空；
- 当 1%≤数值＜50%时，进度条为绿色；
- 当 50%≤数值＜70%时，进度条为黄色；
- 当数值≥70%时，进度条为红色。

4. 上述三个参数显示了设备接近于满负荷运行的程度。如果它们的值都比较低，就表明设备还有能力处理比它现在所运行的更多的网络通讯。如果它们的值都很高，就表明设备已经接近于满负荷工作，此时再增加更多的任务可能会导致系统对通讯的处理出现延迟。

10.6.4 系统版本信息

图 10-13 系统版本信息

- 序列号：产品的内部序列号（和表面序列号可能不同）；
- 功能号：产品具有的功能模块；
- 软件版本：产品的软件版本号。

10.6.5 系统端口状态

端口	状态	外出/进入速率(kbit/s)
lan1	100M Full MDI-X	26 / 3
lan2	DOWN	
lan3	DOWN	
lan4	DOWN	

端口	状态	外出/进入速率(kbit/s)
wan1	100M Full MDI	2 / 53

表 10-1 系统的端口状态

- 端口：其中，LAN 接口有 4 个端口；
- 状态：若某端口未激活，其“状态”显示为 DOWN；若已经激活，则依次显示该端口的工作速率、工作状态（Full-全双工，Half-半双工）以及工作模式（MDI-正接，MDI-X-反接）；
- 外出/进入速率（kbit/s）：相关速率是针对接口统计的，即 LAN 口按照 1 个 LAN 口来统计，各个 WAN 口分别统计。

附录 A 配置局域网中的计算机

本章讲述如何在 Windows XP 环境下配置计算机的 TCP/IP 属性。

第一步 检查网络 IP 状态

1. 单击“开始”→“控制面板”→“网络和 Internet 连接”;

2. 双击“网络连接”图标，右键单击“本地连接”图标选择“属性”进入本地连接的属性窗口，在“常规”选项卡中的“此连接使用下列项目”中查看是否已安装了 TCP/IP 协议，如图 A-1 所示，如果出现了“Internet 协议（TCP/IP）”选项，就表示已经安装：

图 A-1 网络配置窗口

3. 如果没有安装 TCP/IP 协议，在“本地连接 属性”窗口单击“安装”按钮，随后单击“协议”→“添加”→“Microsoft”→“TCP/IP 传输协议”即可。在指定的网卡完成添加 TCP/IP 协议后，需重启计算机来更新系统的网络设定，使其生效。

第二步 配置 TCP/IP 属性

下面分别介绍手工设置 IP 地址和通过 DHCP 服务器设置 IP 地址这两种情形下，配置 TCP/IP 属性的步骤。

方法一 手工设置 IP 地址

1. 单击“开始”→“控制面板”→“网络和 Internet 连接”；

2. 双击“网络连接”图标，右键单击“本地连接”图标选择“属性”进入本地连接的属性窗口，在“常规”选项卡中的“此连接使用下列项目”选择“Internet 协议（TCP/IP）”，再单击“属性”按钮；

3. 进入“Internet 协议（TCP/IP）属性”窗口，如图 A-2 所示，首先选中“使用下面的 IP 地址”选项，然后在“IP 地址”中填入：192.168.16.X（X 在 2 至 254 之间），在“子网掩码”中填入 255.255.255.0；在“默认网关”中填入设备的 LAN 口 IP 地址（出厂时为 192.168.16.1）；在首选 DNS 服务器和备选 DNS 服务器填入 ISP 提供的 DNS 地址，备用 DNS 服务器为选填，单击“确定”按钮，保存配置。

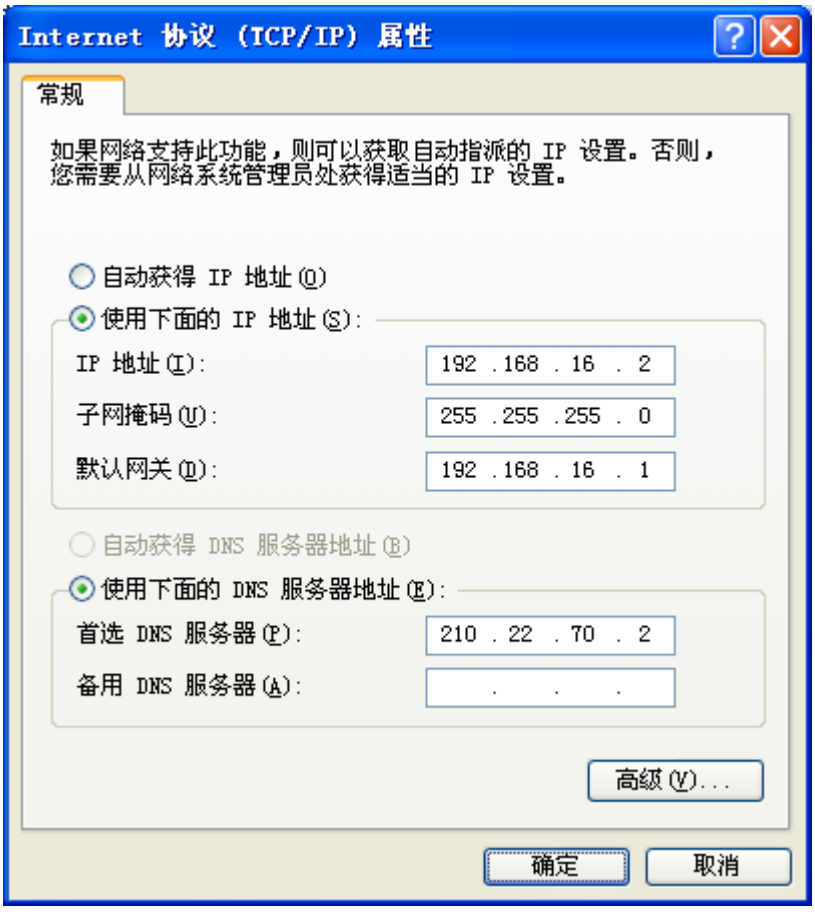

Internet 协议 (TCP/IP) 属性
常规
如果网络支持此功能，则可以获取自动指派的 IP 设置。否则，您需要从网络系统管理员处获得适当的 IP 设置。
自动获得 IP 地址(O)
使用下面的 IP 地址(S):
IP 地址(I): 192 . 168 . 16 . 2
子网掩码(U): 255 . 255 . 255 . 0
默认网关(D): 192 . 168 . 16 . 1
自动获得 DNS 服务器地址(B)
使用下面的 DNS 服务器地址(E):
首选 DNS 服务器(P): 210 . 22 . 70 . 2
备用 DNS 服务器(A):
高级(V)...
确定
取消

图 A-2 INTERNET 协议（TCP/IP）属性 IP 地址配置窗口

方法二 通过 DHCP 服务器设置 IP 地址

1. 使用此功能之前，必须确保已经在设备的***基本配置—>DHCP 和 DNS 服务器***中激活 DHCP Server 功能（章节 5.2.1）；

2. 单击“开始”→“控制面板”→“网络和 Internet 连接”；

3. 双击“网络连接”图标，右键单击“本地连接”图标选择“属性”进入本地连接的属性窗口，在“常规”选项卡中的“此连接使用下列项目”选择“Internet 协议（TCP/IP）”，再单击“属性”按钮；

4. 进入“Internet 协议（TCP/IP）属性”窗口，选中“自动获得 IP 地址”和“自动获得

DNS 服务器地址”，单击“确定”按钮，保存配置，如图 A-3 所示：

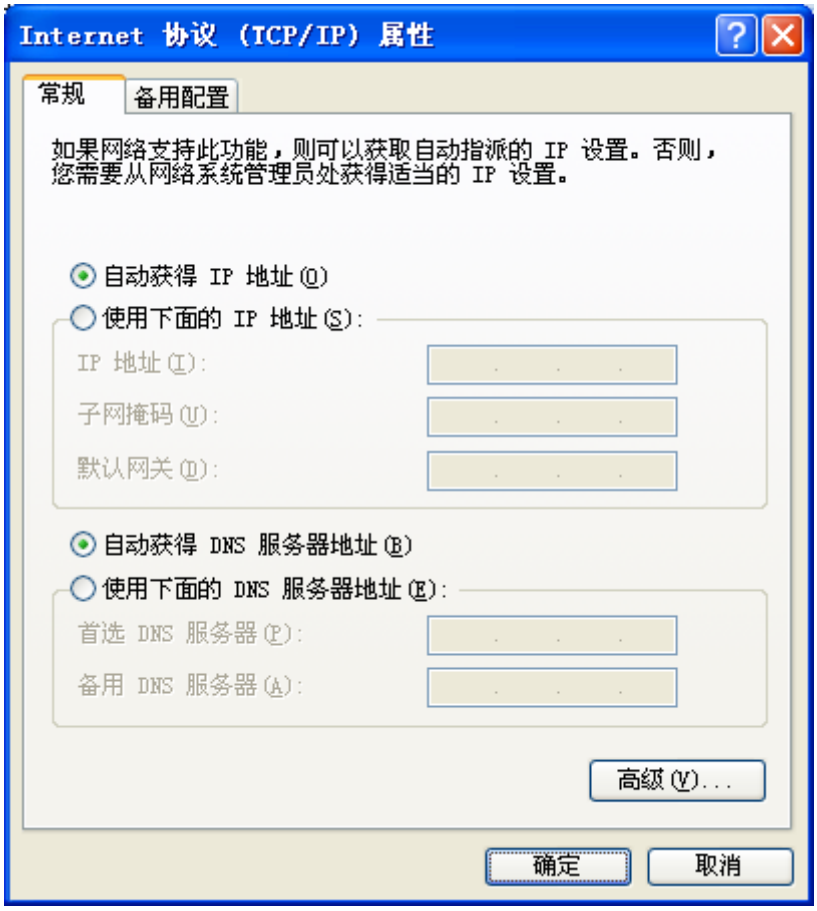


图 A-3 TCP/IP 属性 IP 地址配置窗口

附录 B FAQ

1. ADSL 用户如何上网？

1) 首先，将 ADSL Modem 设置为桥模式（1483 桥模式）；

2) 确认 PPPoE 线路是标准拨号型的（可以使用 WindowsXP 自带 PPPoE 软件拨号测试）；

3) 用网线将设备的 WAN 口与 ADSL Modem 相连，并将电话线连接到 ADSL Modem 的 Line 口；

4) 在***基本配置—>线路配置***中，配置 PPPoE 上网线路的相关参数（章节 5.1.2.1）；

5) 若是包月上网的用户，则可选择拨号类型为“自动拨号”。若是非包月上网的用户，则可选择拨号类型为“按需拨号”或者“手动拨号”，并且可以输入空闲时间，以防止忘记断线而浪费上网时间；

6) 若选择了“手动拨号”，则需在***基本配置—>线路配置***的“线路连接信息列表” （章节 5.1.1）中进行手动拨号；

7) 拨号成功后，在***基本配置—>线路配置***的“线路连接信息列表”中可以查看该线路的配置和状态信息（如表 B-1、B-2），比如“连接状态”（拨号成功后显示为“已连接”）、ISP 分配的“IP 地址”等信息。

线路连接信息列表 1/18

1/1 第一页 上一页 下一页 最后页 前往 第 页 搜索

线路名称	物理接口	连接类型	连接状态	IP地址	子网掩码
默认线路	WAN1	PPPoE(Ad21564255)(普通模式)	已连接(持续:00:00:01:31)	10.0.0.29	255.255.255.

拨号 挂断 刷新

表 B-1 线路连接信息列表——查看 PPPoE 拨号线路信息

表 B-2 线路连接信息列表——查看 PPPoE 拨号线路信息（续表 B-1）

8) 按照本手册附录 A 所述内容配置局域网计算机。

2. 固定 IP 接入用户如何上网？

1) 确认线路正常（可以使用计算机测试）；

2) 用网线将设备的 WAN 口与 ISP 网络设备相连；

3) 在***基本配置—>快速向导***或***基本配置—>线路配置***中，配置固定 IP 接入线路的相关参数；

4) 按照本手册附录 A 所述内容配置局域网计算机。

3. 动态 IP（Cable Modem）接入用户如何上网？

1) 确认线路正常（可以使用计算机测试）；

2) 用网线将设备的 WAN 口与 ISP 网络设备相连；

3) 在***基本配置—>快速向导***或***基本配置—>线路配置***中，配置动态 IP 接入线路的相关参数；

提示：某些动态 IP 接入的时候（比如有线通），Cable Modem 会记录下原先使用该线路的网络设备（如网卡）的 MAC 地址，这样会导致设备无法正常获得 IP 地址，此时需要将设备的 WAN 口 MAC 地址设置成和原有网络设备的 MAC 地址相同。在***基本配置—>线路配置***中，选择“连接类型”为“动态 IP 接入”，配置“广域网接口 MAC 地址”，单击“保存”按钮，重启设备后配置生效。

4) 在***基本配置—>线路配置***的“线路连接信息列表”中，可以查看动态 IP 接入时线路的配置和状态信息（如表 B-6、表 B-7），比如“连接状态”（正常连接时显示为“已连接”，并显示剩余租用时间）、ISP 分配的“IP 地址”、“网关地址”等信息。

线路连接信息列表
1/18
1/1 第一页 上一页 下一页 最后页 前往 第 页 搜索
线路名称 物理接口 连接类型 连接状态 IP地址 子网掩码
默认线路 WAN1 动态IP 已连接(剩余:00:00:59:59) 192.168.16.118 255.255.255.0
更新 释放 刷新

表 B-6 线路连接信息列表——查看动态 IP 接入线路信息

表 B-7 线路连接信息列表——查看动态 IP 接入线路信息（续表 B-6）

5) 按照本手册附录 A 所述内容配置局域网计算机。

4. 如何将设备恢复到出厂配置?

提示：下述方法将删除设备原来所有配置，请谨慎使用。

下面介绍将设备恢复到出厂配置的方法，按知道管理员密码和忘记管理员密码分别说明（注：本节中均以 Windows XP 环境为例进行说明）。

情况一：知道管理员密码

当用户知道管理员密码时，可以通过 WEB 界面来恢复出厂配置。

步骤如下：直接进入***系统管理—>配置管理***页面，在“恢复出厂配置”配置栏中，单击“恢复”按钮，即可恢复出厂值。

情况二：忘记管理员密码

如果忘记了管理员密码，将无法进入 WEB 界面，可以通过 RESET 按钮来恢复设备的出厂配置。

步骤如下：在设备带电运行过程中，按住 Reset 按钮 5 秒钟以上，再松开此按钮，设备将恢复到出厂配置，并自动重启。

附录 C 图索引

图 0-1 DNS 服务器配置 3
图 0-2 DNS 服务器配置 4
图 2-1 建立局域网和广域网连接——HIPER 510 12
图 2-2 系统指示灯——HIPER 510 13
图 2-3 建立局域网和广域网连接——HIPER 520 14
图 2-4 系统指示灯——HIPER 520 14
图 3-1 WEB 登录界面 18
图 3-2 WEB 界面首页 19
图 3-3 开始菜单的子菜单 19
图 3-4 提示信息 20
图 3-5 双线路路由配置 20
图 3-6 病毒防御 21
图 3-7 页面刷新功能配置 22
图 3-8 系统运行时间 22
图 3-9 系统资源状态 22
图 3-10 系统版本信息 23
图 3-11 快捷图标 24
图 3-12 网站知识库超链接 24
图 4-1 上网接入方式设置 25
图 4-2 PPPOE 拨号上网方式 26
图 4-3 PPPOE 拨号配置 27
图 4-4 固定 IP 接入方式 28
图 4-5 固定 IP 接入配置 28
图 4-6 动态 IP 接入方式 29
图 4-7 动态 IP 接入配置 29
图 5-1 PPPOE 拨号上网线路配置 36
图 5-2 固定 IP 接入线路配置 38
图 5-3 动态 IP 接入线路配置 40
图 5-4 删除线路 40
图 5-5 对话框——删除线路 41
图 5-6 线路组合通用配置——所有线路负载均衡 45
图 5-7 线路组合配置——部分线路负载均衡，其余备份 45
图 5-8 线路检测及权重配置 46
图 5-9 DHCP 服务配置 50
图 5-10 接口配置 53
图 5-11 申请 DDNS 帐号 56
图 5-12 配置 DDNS 服务 57
图 6-1 对称 NAT 简介 60
图 6-2 端口映射配置 60

图 6-3 端口映射配置——实例一 62
图 6-4 NAT 全局配置 62
图 6-5 对称 NAT 配置 62
图 6-6 静态路由配置 65
图 6-7 静态路由配置——实例一 67
图 6-8 静态路由配置——实例二 68
图 6-9 IP/MAC 地址绑定配置 71
图 6-10 IP/MAC 绑定全局配置 72
图 6-11 UPNP 配置 78
图 6-12 即插即用设置 80
图 7-1 DISCOVERY 阶段的基本工作流程 81
图 7-2 PPPOE 服务器全局配置 83
图 7-3 用户配置 84
图 7-4 PPPOE 服务器全局配置——实例 85
图 7-5 PPPOE 账号 A 配置——实例 86
图 7-6 PPPOE 账号 B 配置——实例 86
图 7-7 PPPOE 账号 C 配置——实例 86
图 8-1 全局限速配置 87
图 8-2 特殊用户地址组配置——实例 89
图 8-3 带宽管理配置——实例 89
图 8-4 创建地址组 90
图 8-5 时间段配置 92
图 8-6 日期设置——时间段设置 93
图 8-7 时间段详细信息 94
图 8-8 时间段 WORKTIME 配置——实例 96
图 8-9 时间段 FREETIME 配置——实例 97
图 9-1 上网行为管理设置 100
图 9-2 只允许 WEB 访问 102
图 9-3 上网行为管理实例配置——策略 1 104
图 9-4 上网行为管理实例配置——策略 2 106
图 9-5 上网行为管理实例配置——策略 3 106
图 9-6 域名过滤配置 106
图 9-7 域名过滤全局配置 107
图 9-8 策略库版本检查 109
图 9-9 导入策略库 110
图 10-1 管理员配置 111
图 10-2 时钟管理配置 112
图 10-3 显示和保存当前软件 113
图 10-4 软件升级 113
图 10-5 恢复出厂配置 115
图 10-6 重启设备 115
图 10-7 提示信息 115
图 10-8 设备重启中 116
图 10-9 远程管理 117

图 10-10 页面刷新功能配置 118
图 10-11 系统运行时间 118
图 10-12 系统资源状态 118
图 10-13 系统版本信息 119

附录 D 表索引

表 0-1 端口映射列表 2
表 0-2 DHCP 地址使用信息列表 3
表 0-3 接口出厂配置 4
表 2-1 第一组指示灯 13
表 2-2 第二组指示灯 13
表 2-3 第一组指示灯 15
表 2-4 第二组指示灯 15
表 3-1 系统的端口状态 23
表 5-1 线路连接信息列表 31
表 5-2 线路连接信息列表（续表 5-1） 32
表 5-3 PPPoE 拨号线路连接状态描述 32
表 5-4 固定 IP 接入线路连接状态描述 33
表 5-5 动态 IP 接入线路连接状态描述 33
表 5-6 线路连接信息列表——PPPoE 拨号接入 34
表 5-7 线路连接信息列表——PPPoE 拨号接入（续表 5-6） 34
表 5-8 线路连接信息列表——动态 IP 接入 35
表 5-9 线路连接信息列表——动态 IP 接入（续表 5-8） 35
表 5-11 线路组合信息列表 47
表 5-12 线路组合信息列表（续表 5-11） 47
表 5-12 DHCP 地址使用信息列表 51
表 5-13 接口配置信息列表 54
表 5-14 DDNS 状态 57
表 6-1 端口映射列表 61
表 6-2 系统保留的缺省路由名 64
表 6-3 系统保留的检测路由名 65
表 6-3 路由信息列表 66
表 6-4 IP/MAC 绑定信息列表——实例一 70
表 6-5 IP/MAC 绑定信息列表——实例二 71
表 6-6 IP/MAC 绑定信息列表 73
表 6-7 IP/MAC 绑定信息列表——实例三 75
表 6-8 IP/MAC 绑定信息列表——实例四 76
表 6-9 IP/MAC 绑定信息列表——实例五 76
表 6-10 IP/MAC 绑定信息列表——实例六 77
表 6-11 UPnP NAT 映射列表 79
表 6-12 UPnP NAT 映射列表 79
表 7-1 PPPoE 用户状态信息列表 84
表 7-2 PPPoE 用户状态信息列表——实例 86
表 8-1 用户带宽使用列表 88
表 8-2 地址组信息列表 91

表 8-3 时间段信息列表.....94
表 9-1 上网行为管理列表.....101
表 9-2 上网行为管理（续表 9-1）.....101
表 9-3 策略库信息列表.....108
表 10-1 系统的端口状态.....119